R E P U B L I Q U E F R A N C A I S

PCT / IB 0 0 / 0 1 3 1 2

15. 12. 00

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

4

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 07 NOV. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

M Haut

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☒

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 05/10/99.

N° D'ENREGISTREMENT NATIONAL 9913401

DÉPARTEMENT DE DÉPÔT 99

DATE DE DÉPÔT 05 OCT. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Georges CORNUEJOLS
2, impasse Bellevue
31450 AYGUESVIVES

n°du pouvoir permanent | références du correspondant | téléphone

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale : ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☒ différé ☐ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Procédé et dispositif de communication pour la sécurisation des informations

3 DEMANDEUR (S) n° SIREN | code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

CORNUEJOLS GEORGES
CORNUEJOLS THEBAULT EMMANUELLE

Forme juridique

Nationalité (s) FRANCAISE

Adresse (s) complète (s) Pays

2, impasse Bellevue
31450 AYGUESVIVES

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☒ oui ☐ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
FRANCE	99 11250	31/08/99	BREVET D'INVENTION

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Georges Cornuéjols

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
51,52				14/03/2000	FA-16 MAI 2000
27				27/3/2000	FA-11 SEPT. 200

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

La présente invention concerne un procédé et un dispositif de communication. Plus particulièrement, la présente invention s'applique à sécuriser des données, des communications ou des transactions en ligne. Encore plus particulièrement, la présente invention s'attache à sécuriser des transmissions d'informations confidentielles et des achats effectués par l'intermédiaire d'un réseau de communication, par exemple l'Internet.

Un utilisateur d'un réseau de communication, par exemple l'Internet, sent un certain inconfort lorsqu'il s'aventure sur ce réseau. Il ne peut garder de traces organisées des pages informatiques qu'il reçoit, il ne peut identifier aisément les personnes, physiques ou morale à qui il a à faire, il se sent en insécurité au cours de ses achats en ligne et finalement, est demandeur d'une assistance semi-automatique.

Selon un premier aspect, la présente invention vise un procédé de sécurisation, caractérisé en ce qu'il comporte :

- une opération de mise en mémoire de caractéristiques de données dites « confidentielles »,
- une opération d'ouverture d'une communication sur un réseau de communication,
- une opération de comparaison de caractéristiques de données à transmettre sur ledit réseau avec lesdites caractéristiques mises en mémoire et
- lorsqu'une caractéristique de données à transmettre correspond à une caractéristique de donnée confidentielle, une opération de retardement de la transmission desdites données à transmettre.

Selon des caractéristiques particulières du procédé visé par le premier aspect de la présente invention, ladite opération de comparaison est effectuée en tâche de fond par rapport à l'opération de communication.

Selon des caractéristiques particulières du procédé visé par le premier aspect de la présente invention, les caractéristiques des données confidentielles sont insuffisantes pour déterminer les données confidentielles protégées.

Selon un deuxième aspect, la présente invention vise un procédé de gestion de mémoire, caractérisé en ce qu'il comporte :

- au moins une opération de communication par l'intermédiaire d'un réseau de communication,

- au moins une opération de mémorisation de différents types de données en provenance dudit réseau au cours de ladite opération de communication,

- une opération de détermination de nécessité d'effacer certaines données mémorisées, et

- lorsqu'il est nécessaire d'effacer des données mémorisées, une opération d'effacement au cours de laquelle des données mémorisées sont effacées en fonction de leur date de mémorisation et de leur type, les données d'au moins un type prédéterminé étant conservées plus longtemps que les données d'au moins un autre type.

Selon des caractéristiques particulières du procédé visé par le deuxième aspect de la présente invention, l'opération de détermination de nécessité comporte une opération de comparaison d'un espace mémoire avec une valeur d'espace mémoire prédéterminée.

Selon des caractéristiques particulières du procédé visé par le deuxième aspect de la présente invention, ce procédé comporte une opération de comparaison de page déjà mémorisée et de page visitée au cours de l'opération de communication sur un réseau de communication et au cours de l'opération de mémorisation, seules les pages non encore mémorisées sont mémorisées.

Selon un troisième aspect, la présente invention vise un procédé de communication caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une première session de communication avec un premier site d'un réseau de communication,

- une opération d'ouverture d'une deuxième session de communication avec un deuxième site dudit réseau de communication,

- une opération de transmission audit deuxième site d'informations relatives à la première session et

- une opération de réception, en provenance dudit deuxième site, d'informations relatives à la première session.

Selon des caractéristiques particulières du troisième aspect de la présente invention, ladite opération de transmission audit deuxième site comporte une opération de transmission automatique d'un identifiant dudit premier site.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, le procédé de communication comporte une opération de mémorisation d'au moins

une caractéristique d'une information confidentielle et ladite opération d'ouverture d'une deuxième session de communication comporte une opération de détection d'une caractéristique d'une information confidentielle dans des données à transmettre audit premier site.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, le procédé de communication comporte une opération de transmission audit premier site d'informations basées sur des informations reçues en provenance dudit deuxième site.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, les informations reçues en provenance du deuxième site comporte une racine ou code générateur d'un identificateur de moyen de paiement.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, le procédé de communication comporte une opération de transmission dudit identificateur de moyen de paiement audit premier site.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, l'opération de transmission audit deuxième site d'informations relatives à la première session comporte une opération de transmission d'un identifiant d'un produit ou service susceptible d'être fourni par l'intermédiaire dudit premier site.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, le procédé de communication comporte une opération de mémorisation automatique de données reçues de la part du premier site au cours de ladite première session.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, le procédé de communication comporte une opération de requête d'informations permettant de déterminer un identificateur de moyen de paiement à usage unique.

Le du troisième aspect de la présente invention vise aussi un procédé de communication caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication dite « deuxième » avec un terminal,

- une opération de réception en provenance dudit terminal d'une information relative à une session de communication dite « première » à laquelle participe ledit terminal et

- une opération de fourniture audit terminal d'informations relatives à la première session.

Selon des caractéristiques particulières du troisième aspect de la présente invention, les informations relatives à la première session comporte une racine ou code générateur permettant de définir un identificateur de moyen de paiement à usage unique.

Selon d'autres caractéristiques particulières du troisième aspect de la présente invention, le procédé de communication comporte une opération de réception dudit identificateur, une opération de vérification de validité dudit identificateur, une opération de déclenchement de paiement et une opération d'invalidation dudit identificateur.

Selon un quatrième aspect, la présente invention vise un procédé paiement en ligne, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une première session de communication avec un premier site, par l'intermédiaire d'un réseau de communication,
- une opération de réception d'une racine d'un identificateur de moyen de paiement à usage unique, de la part dudit premier site,
- une opération de détermination d'un identificateur de moyen de paiement à usage unique,
- une opération de fourniture dudit identificateur à un deuxième site, par l'intermédiaire dudit réseau de communication, au cours d'une deuxième session de communication, et
- une opération paiement par ledit moyen de paiement à usage unique.

En relation avec le quatrième aspect, la présente invention vise un procédé de paiement caractérisé en ce qu'il comporte :

- une opération de génération d'une racine d'un identificateur de moyen de paiement à usage unique,
- une opération de transmission de ladite racine à un utilisateur, par l'intermédiaire d'un réseau de communication,
- une opération de réception d'un identificateur de moyen de paiement à usage unique de la part d'un tiers,
- une opération de vérification de correspondance dudit identificateur avec ladite racine,

et lorsqu'il y a correspondance :

- une opération de paiement dudit tiers, au débit dudit utilisateur, et
- une opération d'invalidation dudit moyen de paiement à usage unique à la suite de la première opération de paiement utilisant ledit moyen de paiement.

Selon des caractéristiques particulières du procédé visé par le quatrième aspect de la présente invention, ce procédé comporte une opération d'authentification de l'utilisateur.

Selon des caractéristiques particulières du procédé visé par le quatrième aspect de la présente invention, cette opération d'authentification comporte une opération de reconnaissance d'un identificateur d'un moyen de paiement à usage permanent.

Selon des caractéristiques particulières du procédé visé par le quatrième aspect de la présente invention, l'identificateur de moyen de paiement à usage unique est un identificateur de carte de paiement, par exemple à 20 chiffres compris entre 0 et 9.

Selon des caractéristiques particulières du procédé visé par le quatrième aspect de la présente invention, l'opération d'ouverture de la deuxième session précède l'opération d'ouverture de la première session.

Selon des caractéristiques particulières du procédé visé par le quatrième aspect de la présente invention, l'opération de paiement comporte une opération de vérification d'un identifiant du deuxième site.

Selon un cinquième aspect, la présente invention vise un procédé de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une première session de communication entre un terminal et un site d'un réseau de communication,
- une opération de sélection d'une date,
- une opération de mémorisation de ladite date et,
- à ladite date, une opération d'ouverture automatique d'une deuxième session de communication entre ledit terminal et ledit site.

Selon des caractéristiques particulières du procédé visé par le cinquième aspect de la présente invention, ce procédé comporte une opération d'interrogation d'un utilisateur dudit terminal et ladite deuxième session dépend d'au moins une réponse donnée par ledit utilisateur.

Selon un sixième aspect, la présente invention vise un procédé de mémorisation de communications, caractérisé en ce qu'il comporte une opération de mémorisation de contenus de pages accessibles par l'intermédiaire d'un réseau de communication et une opération de relecture de contenu mémorisé comportant une opération de sélection de vitesse de relecture et, lorsqu'une vitesse de relecture lente est sélectionnée, une première opération d'affichage de contenu mémorisé pendant une première durée, et lorsqu'une vitesse de relecture rapide est

sélectionnée, une deuxième opération d'affichage de contenu mémorisé pendant une deuxième durée inférieure à la première durée.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, lorsqu'une fonction de relecture lente est sélectionnée, au cours de la première opération d'affichage, une première portion de contenu mémorisé est affichée et, au cours de la deuxième opération d'affichage, une deuxième portion de contenu mémorisé est affichée la deuxième portion étant différente de la première portion.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, la deuxième portion comporte au moins une adresse de page accessible sur le réseau de communication.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, la deuxième portion comporte au moins une date de mémorisation.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, la deuxième portion comporte un contenu de haut de page accessible sur le réseau de communication.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, le procédé comporte une opération d'affichage de parties de pages accessibles et la première portion comporte une opération de réaffichage des parties de pages déjà affichées, dans l'ordre de leur premier affichage au cours de l'opération d'affichage.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, au cours de l'opération de mémorisation, l'utilisateur sélectionne les pages à mémoriser.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, le procédé comporte, avant l'opération de relecture, une opération d'authentification de l'utilisateur.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, la première portion comporte la deuxième portion.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, la première opération de relecture est automatique, chaque élément de l'information mémorisée et affichée ne restant pas affichée pendant plus d'une durée prédéterminée.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, le procédé comporte une opération de sélection de touches affichées dans une barre d'outil sur un écran de visualisation où sont affichées les portions de contenu.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, le procédé comporte une opération d'arrêt de relecture et, à la suite de l'opération d'arrêt de relecture, une opération d'affichage de tout le contenu mémorisé relatif à la page en cours d'affichage au moment de la sélection de l'arrêt de relecture.

Selon des caractéristiques particulières du sixième aspect du procédé visé par la présente invention, le procédé comporte une opération de sélection d'ordre de relecture au cours de laquelle l'utilisateur sélectionne une ordre de défilement de page identique à l'ordre de mémorisation ou un ordre de défilement de page inverse à l'ordre de mémorisation.

Selon un septième aspect, la présente invention vise un procédé de mémorisation de communications, caractérisé en ce qu'il comporte une opération de réception de pages en provenance d'un réseau de communication, une opération d'affichage de pages reçues, une opération de sélection de groupe de pages, une opération de mémorisation de contenus de dites pages en relation avec le groupe sélectionné, une opération de sélection de groupe de pages et une opération de réaffichage de pages mémorisées en relation avec le groupe sélectionné.

Selon un huitième aspect, la présente invention vise un procédé de transmission d'une page sur un réseau de communication, caractérisé en ce qu'il comporte:

- une première opération de requête de transmission d'un premier contenu de ladite page correspondant à une première quantité d'information à transmettre et, en cas d'échec de la transmission pour cause de dépassement d'une durée de transmission prédéterminée,

- une opération de détermination automatique d'un deuxième contenu de ladite page, le deuxième contenu correspondant à une quantité d'information à transmettre inférieure à la première quantité et une opération de requête de transmission dudit deuxième contenu de ladite page.

Selon des caractéristiques particulières du procédé visé par le huitième aspect de la présente invention, le deuxième contenu est une partie du premier contenu.

Selon des caractéristiques particulières du procédé visé par le huitième aspect de la présente invention, le deuxième contenu correspond à des fichiers texte.

Selon des caractéristiques particulières du procédé visé par le huitième aspect de la présente invention, le premier contenu correspond à des fichiers représentatifs d'image et/ou de sons.

On observe que la mise en oeuvre du procédé peut être effectuée en tout lieu du réseau de communication, et, en particulier, dans le terminal informatique ou dans un système informatique d'un fournisseur d'accès audit réseau. On observe que le moyen de sécurisation peut aussi se trouver sur le réseau de communication, en tout endroit (à l'exception du site informatique) et, en particulier, dans le terminal informatique ou dans un système informatique d'un fournisseur d'accès audit réseau.

La présente invention vise aussi un site informatique, un serveur, un ordinateur, caractérisé en ce qu'ils mettent en oeuvre le procédé succinctement exposé ci-dessus. La présente invention vise aussi un support d'information, tel qu'une disquette, un disque dur, un compact disque ou une mémoire d'ordinateur, qui conserve des instructions de programme pour :

- ouvrir une session de communication entre un terminal informatique et un site informatique, par l'intermédiaire d'un réseau de communication,

- détecter automatiquement une préparation de paiement par transmission, au cours de ladite session, par l'intermédiaire dudit terminal, d'un identifiant d'un moyen de paiement, et

- lorsqu'une préparation de paiement est détectée, sécuriser automatiquement ledit paiement en dehors dudit site informatique, au moins en sauvegardant le montant du paiement en dehors dudit site informatique.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre, faite dans un but explicatif et nullement limitatif, en regard des dessins annexés dans lesquels :

- la figure 1 représente un mode de réalisation d'un dispositif adapté à la mise en oeuvre du procédé visé par la présente invention,

- la figure 2 représente un organigramme d'un premier mode de mise en oeuvre du premier aspect du procédé visé par la présente invention,

- la figure 3 représente un organigramme d'un deuxième mode de mise en oeuvre du premier aspect du procédé visé par la présente invention,

- la figure 4 représente un organigramme de mise en oeuvre du deuxième et du huitième aspects du procédé visé par la présente invention,

- les figures 5A et 5B représentent un organigramme de mise en oeuvre du sixième aspect de la présente invention;

- la figure 6 représente un écran de visualisation au cours d'une opération de relecture de l'organigramme illustré en figure 5,

- la figure 7 représente un organigramme de mise en oeuvre du troisième aspect du procédé visé par la présente invention,

- la figure 8 représente des fonctions mises en oeuvre dans différents systèmes informatiques reliés à un réseau de communication au cours d'un premier exemple de succession d'opération mises en oeuvre conformément au quatrième aspect du procédé visé par la présente invention,

- la figure 9 représente des fonctions mises en oeuvre dans différents systèmes informatiques reliés à un réseau de communication au cours d'un deuxième exemple de succession d'opérations mises en oeuvre conformément au quatrième aspect du procédé visé par la présente invention.

- la figure 10 représente un écran de visualisation au cours de la mise en oeuvre d'un autre mode de réalisation du procédé objet de la présente invention,

- la figure 11 représente un organigramme de fonctionnement du dispositif illustré en figure 1, selon le mode de réalisation du procédé objet de la présente invention illustré en figure 10,

- la figure 12 représente un organigramme de fonctionnement du dispositif illustré en figure 1, selon un autre mode de réalisation du procédé objet de la présente invention,

- la figure 13 représente un écran de visualisation au cours de la mise en oeuvre du mode de réalisation du procédé objet de la présente invention illustré en figure 12,

- la figure 14 représente un organigramme de fonctionnement de chacun des modes de réalisation illustrés en figures 11 et 12,

- la figure 15 représente un organigramme de fonctionnement d'un aspect particulier de la présente invention,

- la figure 16 représente un organigramme de fonctionnement du dispositif illustré en figure 1, pour la mise en oeuvre du cinquième aspect de la présente invention, et

- la figure 17 représente des fonctions mises en oeuvre dans différents systèmes informatiques reliés à un réseau de communication au cours d'un troisième exemple de succession d'opération mises en oeuvre conformément au quatrième aspect du procédé visé par la présente invention.

Pour certains des aspects de la présente invention, préférentiellement, le procédé est implémenté en tâche de fond pour ne pas perturber le fonctionnement auquel l'utilisateur est habitué, jusqu'à ce qu'un événement de déclenchement survienne, soit volontairement de la part de l'utilisateur, soit par détection d'une information confidentielle à protéger.

Pour chacun des aspects de la présente invention, un logiciel qui le met en oeuvre réside préférentiellement dans le terminal de l'utilisateur ou dans un serveur d'un fournisseur d'accès au réseau concerné.

Chacun des aspects de la présente invention participe à la définition d'un procédé et d'un dispositif d'assistance à un utilisateur d'un réseau de communication. Dans la suite de la description, le terme « logiciel d'assistance » fait référence à un exemple particulier d'implémentation de certains aspects du procédé et du dispositif visé par la présente invention.

En figure 1 sont représentés un terminal informatique 100, connecté, par l'intermédiaire d'un réseau 120, d'un serveur d'un fournisseur d'accès 130 et d'un réseau 140, à un site informatique distant 150. Dans le premier mode de réalisation illustré en figure 1, le terminal 100 comporte, reliés entre eux par un bus d'adresses et de données 109, une interface de communication sur un réseau 101, une unité de sauvegarde non volatile 102, un dispositif de pointage 103, un écran de visualisation 104, un clavier 105, une unité centrale 106, une mémoire centrale non volatile 107 et une mémoire vive 108.

Le réseau 120 est, par exemple, le réseau téléphonique commuté. Le serveur du fournisseur d'accès 130 est, par exemple, le serveur du fournisseur d'accès au réseau Internet connu sous le nom d'AOL (marque déposée) ou de WANADOO (marque déposée). Le réseau 140 est, par exemple, le réseau de communication informatique connu sous le nom d'Internet. Le site informatique distant 150 est mis en oeuvre par un serveur informatique ou un ordinateur programmé à cet effet selon des techniques connues.

Dans le premier mode de réalisation illustré en figure 1, le terminal 100 est un ordinateur personnel connu sous le nom de PC (acronyme de Personal Computer pour ordinateur personnel) ou un ordinateur de réseau, connu sous le nom de NC (acronyme de Network Computer pour ordinateur de réseau). L'interface de communication sur un réseau 101 est, dans le premier mode de réalisation décrit et représenté, un modulateur-démodulateur ou MODEM. L'unité de sauvegarde non volatile 102, est, dans le premier mode de réalisation décrit et représenté, un disque dur ou un lecteur/enregistreur de disques compacts. Le dispositif de pointage 103, est, dans le premier mode de réalisation décrit et représenté, une

souris informatique. L'écran de visualisation 104 est de type connu, par exemple à tube cathodique et compatible avec la norme connue de l'homme du métier sous le nom de SVGA.

Le clavier 105 comporte au moins des touches qui, seules ou en combinaison, permettent de sélectionner des caractères alphanumériques. L'unité centrale 106 est, dans le premier mode de réalisation décrit et représenté, un processeur, par exemple des marques déposées Intel Pentium. La mémoire centrale non volatile 107 conserve les instructions de programme du processeur 106 qui lui permettent de démarrer lorsqu'il commence à être alimenté en électricité. Le mémoire vive 108 est, dans le premier mode de réalisation décrit et représenté, une mémoire cache adaptée à conserver des informations représentatives d'au moins une page reçue de la part d'un site tel que le site informatique distant 150.

Pour la mise en oeuvre de certains aspects de la présente invention, le terminal 100 est relié, par l'intermédiaire du réseau 140 à un site tiers d'assistance ou de protection 170 et/ou à un site tiers de confiance 180. Le site tiers de protection 170 et le site tiers de confiance 180 possèdent, chacun un serveur qui conserve des pages Internet. En variante, au moins l'un de ces sites 170 et 180 est confondu avec celui du fournisseur d'accès 130.

D'une manière générale, selon le premier aspect de la présente invention, lorsqu'un utilisateur met en fonctionnement un système informatique, le logiciel d'assistance qui met en oeuvre certains des aspects de la présente invention est initialisé et fonctionne en tâche de fond. Ensuite, alors que l'utilisateur utilise ce système informatique, le logiciel d'assistance surveille la fourniture d'informations à protéger. Ces informations sont définies par leur forme (voir par exemple l'organigramme illustré en figure 2) ou par leur valeur particulière (voir par exemple l'organigramme illustré en figure 3). Lorsqu'une information a protéger est détectée en tâche de fond, une opération de protection de cette information est effectuée.

La figure 2 représente un organigramme d'un premier mode de mise en oeuvre du premier aspect du procédé visé par la présente invention. A la suite d'une opération 200 de démarrage du terminal 100, au cours d'une opération 201, le logiciel d'assistance est automatiquement démarré.

Au cours de l'utilisation du terminal 100 et de manière connue, l'utilisateur effectue des sélections en mettant en oeuvre la souris 103 ou des saisies de symboles en utilisant le clavier 105.

Au cours d'un test 202, l'unité centrale 106 détermine si un icône spécifique à la mise en oeuvre du premier aspect du procédé visé par la présente invention a été sélectionné par l'utilisateur, ou non. Cet icône spécifique peut être un icône, telle que icône 1070 illustré en

figure 10 et représenté sur l'écran de visualisation 104, soit un icône qui représente une mémoire d'informations personnelles, connue sous le nom anglais de « valet » ou « wallet », dans les logiciels de navigation (ou « browser ») sur Internet.

Lorsque le résultat du test 202 est négatif, au cours d'une opération 203, l'unité centrale 106 détermine si un symbole a été saisi au clavier 105. Lorsque le résultat du test 203 est négatif, le test 202 est réitéré. Lorsque le résultat du test 203 est positif, au cours d'une opération 204, le symbole saisi est mis en mémoire dans un registre « premier entré premier sorti » (connu de l'homme du métier sous l'acronyme anglais FIFO pour First In, First Out) qui possède une dimension au moins égale à la plus grande des séquences de symboles dont la diffusion est protégée. Au cours d'une opération 205, des caractéristiques de reconnaissance de la séquence saisie sont déterminées. Ces caractéristiques de reconnaissance sont des informations qui caractérisent la séquence conservée dans le registre premier entré premier sorti et qui sont destinées à être comparées à des caractéristiques de reconnaissance de séquences protégées.

Par exemple, si l'information protégée est un numéro de sécurité sociale ou un numéro de carte de paiement, des caractéristiques peuvent être constituées du nombre de chiffres entrés consécutivement et de la vraisemblance que certains de ces chiffres représentent un mois, une année, un sexe, une information de redondance par rapport aux autres chiffres ou de toute autre fonction, éventuellement à sens unique, qui fournit au moins une caractéristique.

Par exemple, un numéro de carte de crédit possède 16 chiffres, qui possèdent entre eux une relation, et une date de péremption sous forme de deux chiffres pour le mois et deux chiffres pour l'année, l'année ne pouvant être plus de quelques années après la date d'émission de la carte de crédit. Ceci fournit plusieurs caractéristiques d'un numéro de carte de crédit, sans qu'il soit nécessaire d'identifier ce numéro.

Par exemple, un numéro de sécurité sociale français possède les caractéristiques suivantes (sauf très rares exception):

- il comporte 13 chiffres
- le premier chiffre est égal soit à 1, soit à 2,
- le quatrième chiffre est soit 0, soit 1,
- le cinquième est 1 ou 2 lorsque le quatrième chiffre est 1.

Au cours d'un test 206, l'unité centrale 106 détermine si des caractéristiques déterminées au cours de l'opération 205 correspondent à des caractéristiques d'une information à protéger.

Lorsque le résultat du test 206 est négatif, le test 202 est réitéré. Lorsque le résultat du test 202 ou le résultat du test 206 est positif, au cours d'une opération 207, l'information à protéger dont au moins une caractéristique a été reconnue est protégée.

A cet effet, au cours de l'opération 207, l'utilisateur est interrogé sur la saisie en cours par un affichage d'un message dans une fenêtre représentée sur l'écran de visualisation 104, « Etes-vous en train de saisir XXX » où XXX est remplacé par un nom d'information protégé, par exemple « numéro de carte de paiement, numéro de sécurité sociale, code confidentiel, ..., et l'utilisateur doit choisir de sélectionner soit « oui » soit « non ».

Puis lorsque l'utilisateur a choisi « non », l'opération 207 est achevée et lorsque l'utilisateur a choisi « oui », au moins une des opérations de protection exposés dans la mise en oeuvre des autres aspects de la présente invention est mise en oeuvre (effacement des symboles de l'information à protéger, par exemple par simulation d'entrée de touche d'effacement « backspace », mise en mémoire de la succession d'opération effectuée depuis l'opération 201, mise en relation avec un site tiers de protection 170, authentification de l'utilisateur comme personne autorisée à divulguer l'information à protéger, datation, affichage d'information légales, par exemple).

A la suite de l'opération 207, le test 202 est réitéré et les opérations 202 à 206 se succèdent en tâche de fond, jusqu'à ce que le terminal soit arrêté de manière connue.

La figure 3 représente un organigramme d'un deuxième mode de mise en oeuvre du premier aspect du procédé visé par la présente invention. Ce deuxième mode de réalisation comporte les mêmes opérations que le premier mode, à l'exception de l'opération 201 qui est remplacée par des opérations 301 à 304 et l'opération 205 qui est remplacée par une opération 305.

Au cours de l'opération 301, le logiciel d'assistance est automatiquement mis en fonctionnement et provoque l'affichage par l'écran de visualisation 104, dans une fenêtre de dialogue, d'une question de saisie de nouvelles informations à protéger et de trois réponses possibles que l'utilisateur peut sélectionner par l'intermédiaire de la souris 103, « oui », « non », « ne pas démarrer la surveillance ». Lorsque « ne pas démarrer la surveillance » est mis en oeuvre, une opération d'authentification 302 est effectuée. Si l'utilisateur est authentifié, le fonctionnement du logiciel d'assistance est arrêté. Si l'utilisateur n'est pas authentifié, l'opération 301 est réitérée. Lorsque « non » est sélectionné, le test 202 est effectuée. Lorsque « oui » est sélectionné, au cours d'une opération 303, l'utilisateur est invité à saisir un identifiant de l'information à protéger (par exemple en sélectionnant « valet » ou

« walet », « carte de paiement », « numéro de sécurité sociale », « nom », « numéro de permis de conduire », « numéro de carte d'identité », « date de naissance », « adresse », « code d'accès à Internet », « code d'accès au compte bancaire », « autre » ...), puis, une partie des informations à protéger, par exemple les huit premiers chiffres des cartes de paiement à protéger, les six premiers chiffres de son numéro de sécurité sociale, le jour et le mois de sa naissance, les premières lettres de la rue où il habite, les premiers chiffres de son code postal, ...

Puis, au cours d'une opération 304, des caractéristiques de reconnaissance de l'information à protéger sont déterminées de la même manière qu'au cours de l'opération 305 et ces caractéristiques sont mises en mémoire non volatile 102. A la suite de l'opération 304, l'opération 301 est réitérée.

On observe que ces caractéristiques peuvent être constituées de l'intégralité de l'information à protéger, en particulier lorsque l'identification d'information à protéger « autre » a été sélectionnée. Les caractéristiques peuvent aussi être constituées d'un nombre prédéterminé de premiers chiffres du numéro protégé ou de toute autre fonction, éventuellement à sens unique, qui fournit au moins une caractéristique. Le lecteur pourra s'inspirer des procédés de production de redondances pour la correction d'erreurs de transmission (connu sous l'acronyme anglais de FEC pour Forward Error Correction), par exemple les sommes de vérifications connues sous le nom anglais de « checksum ».

Pour les informations conservées dans le registre « valet » ou « wallet », l'utilisateur fournit le nom du logiciel de navigation qu'il utilise ou le met en oeuvre et sélectionne « valet » ou « wallet », de telle manière que l'adresse mémoire à protéger ou le moyen d'y accéder soit déterminé automatiquement par le logiciel d'assistance.

Au cours de l'opération 305, des caractéristiques de reconnaissance de la séquence de symboles en mémoire sont déterminées de la même manière qu'au cours de l'opération 304.

On observe ici que seulement deux moyens d'entrée de données sont mis en oeuvre en figures 2 et 3. Cependant, d'autres moyens d'entrée de données, comme un microphone associé à une logiciel de reconnaissance de la parole, comme un scanner associé à un logiciel de reconnaissance optique de caractères, comme une caméra peuvent être mis en oeuvre conformément au premier aspect de la présente invention.

On observe aussi que les informations à protéger peuvent prendre d'autres formes qu'une séquence de symboles, comme par exemple, une image de fond de l'oeil, une signature

vocale, une signature saisie par utilisation de la souris, une empreinte lue par un capteur optique ou thermique, ...

Dans une variante non représentée, les opérations 201 à 207 ne sont mises en oeuvre automatiquement que lorsque une communication est mise en oeuvre. Ainsi, lorsque des enfants accèdent à un site informatique, par exemple par l'intermédiaire de l'Internet, des informations confidentielles sont protégées.

D'une manière générale, selon le deuxième aspect de la présente invention, des contenus de fichiers informatiques reçus sur un réseau de communication sont mis en mémoire et cet espace mémoire est géré de manière à prévenir qu'il sature l'espace mémoire total disponible pour les autres applications. La mise en mémoire et l'effacement des contenus reçus sur le réseau est hiérarchisé.

D'une manière générale, selon le huitième aspect de la présente invention, lorsque la transmission d'un ensemble d'information échoue à cause d'une limitation de la bande passante disponible ou de la durée de transmission maximale autorisée pour un ensemble, une requête de transmission d'un sous-ensemble dudit ensemble comportant strictement moins d'information que l'ensemble, est automatiquement émise. Préférentiellement, l'ensemble correspond à plusieurs fichiers et le sous-ensemble comporte un ou plusieurs desdits fichiers.

La figure 4 représente un organigramme de mise en oeuvre du deuxième aspect du procédé visé par la présente invention, dans lequel un espace mémoire est géré.

Au cours d'une opération 400, l'utilisateur provoque l'ouverture d'une session de communication entre le terminal 100 et le fournisseur d'accès 130, par l'intermédiaire du réseau 120, de manière connue. Au cours d'une opération 401, le logiciel d'assistance provoque l'affichage d'une fenêtre de sélection et d'un menu comportant un ou plusieurs sujets que l'utilisateur a déjà choisi et/ou une option de définition d'un nouveau sujet. L'utilisateur choisi l'un des sujets affichés et/ou identifie un nouveau sujet. Par exemple, ces sujets peuvent être « bourse », « sport », « voitures », « matériels audiovisuels », « autres » .... Dès que l'utilisateur a sélectionné un sujet, la fenêtre de sélection est effacée de l'écran de visualisation 104.

Puis, au cours d'une opération 402, l'utilisateur sélectionne, de manière connue ou en partant de l'une des pages déjà mises en relation avec le sujet qu'il a sélectionné (A cet effet, lorsque l'utilisateur a choisi un sujet, il peut sélectionner et voir afficher une liste des dernières pages visitées en relation avec le sujet choisi, de la même manière que les logiciels de navigation offrent une liste de sites dit « favoris ». L'utilisateur peut alors cliquer sur une

adresse affichée), une page Internet qu'il souhaite visualiser et une requête est transmise, par l'intermédiaire du fournisseur d'accès 130 à un site qui conserve les informations relatives à la page sélectionnée.

Le site en question transmet ces informations au terminal 100, par l'intermédiaire du réseau 120. En général, la transmission est effectuée avec une bande passante limitée en fonction du trafic existant sur le réseau. Il arrive alors que le fournisseur d'accès arrête la transmission lorsqu'une durée prédéterminée est dépassée. Par exemple, lorsqu'à la fin d'une durée de 20 secondes, les informations relatives à la structure de la page n'ont pas été transmises, le fournisseur d'accès transmet un message d'échec de transmission. Au cours du test 403, l'unité centrale 106 détermine si un tel message a été reçu. Lorsque le résultat du test 403 est positif, c'est-à-dire en cas d'échec de la transmission de la page, au cours d'une opération 404, la transmission d'une partie du contenu de la page est désactivé, la requête de transmission de la page est retransmise et le test 403 est réitéré.

Par exemple, si, pour la même page, plusieurs échecs de transmission se succèdent, les contenu suivants sont successivement désactivés :

- fichiers image animée (par exemple fichiers MPEG),
- fichiers image fixe (par exemple fichiers JPEG),
- fichiers sons (par exemple fichiers WAVE),
- fichiers graphiques.

Selon un autre exemple, le contenu de la page étant décrit au format MPEG-7, les fichiers désactivés sont classés en fonction de leur contenu.

Selon un troisième exemple, les fichiers désactivés comportent, à chaque itération de l'opération 404, le fichier de plus grande dimension, à l'exception du fichier qui donne la structure de la page et/ou du fichier texte.

Lorsque le résultat du test 403 est négatif, au cours de l'opération 405, au moins une partie du contenu de la page sélectionnée est reçue et les désactivations effectuées au cours de l'opération 404 sont annulées pour la prochaine page à recevoir.

Au cours du test 406, l'unité centrale 106 détermine si la page reçue est différente de toutes les pages conservées en mémoire du terminal 100. A cet effet, l'unité centrale 106 compare l'adresse de la page ainsi que la dimension de chaque fichier à cette page avec l'adresse de toutes les pages conservées en mémoire et la dimension des fichiers mémorisés qui sont relatifs à ladite adresse, si elle est reconnue.

Lorsque la page n'est pas reconnue comme mémorisée, le résultat du test 407 est positif et, au cours d'une opération 407, l'unité centrale 106 provoque la mémorisation de tous les fichiers associés à la page reçue, en relation avec l'adresse de la page, dans le disque dur 102.

Lorsque le résultat du test 406 est négatif, c'est-à-dire si la page reçue est reconnue comme déjà mémorisée, ou à la suite de l'opération 407, au cours d'une opération 408, l'unité centrale 106 mémorise, en relation avec ladite page mémorisée, la date, le sujet sélectionné au cours de l'opération 401, ainsi qu'un lien avec la page précédemment sélectionnée au cours de la même session de communication avec le site qui conserve les informations relatives à la page sélectionnée, s'il l'opération 408 n'est pas effectuée pour la première fois au cours de cette session.

Au cours d'une opération 409, au moins une partie de la page reçue est affichée, selon des techniques connues et l'utilisateur peut déplacer cette page, mettre fin à la session de communication, et plus généralement utiliser toutes les fonctions de son logiciel de navigation.

Au cours d'un test 410, l'unité centrale 106 détermine si une autre page a été sélectionné par l'utilisateur, ou non. Lorsque le résultat du test 410 est positif, une requête de transmission est émise à destination du site qui conserve les informations relative à la nouvelle page sélectionnée, avec validation de la transmission de tous les fichiers attachés à ladite page et le test 403 est effectué.

Lorsque le résultat du test 410 est négatif, au cours d'un test 411, l'unité centrale 106 détermine si la mémoire allouée par l'utilisateur pour la conservation de contenus de pages reçues par le réseau de communication 120 est dépassé, ou non.

On observe ici qu'au cours de l'installation du logiciel d'assistance, l'utilisateur alloue un espace mémoire du disque dur 102 à la mémorisation de contenu de pages.

Lorsque le résultat du test 411 est négatif, l'opération 409 est réitérée. Lorsque le résultat du test 411 est positif, au cours d'une opération 412, les fichiers les plus anciens conservés dans l'espace mémoire allouée à la conservation des pages reçues sont triés en fonction de critères prédéterminés et certains fichiers qui ne respectent pas lesdits critères sont effacés.

A titre d'exemple, l'utilisateur peut attribuer à certaines pages, une interdiction d'effacement automatique (voir, par exemple, l'opération 519, en figure 5B) et les fichiers qui

ont dotées de cette interdiction ne sont pas effacés automatiquement. Au cas où tous les fichiers mémorisés sont dotées de cette interdiction, l'utilisateur est avertis qu'il doit :

- soit alloué un complément d'espace mémoire à la fonction de mémorisation de pages reçues par l'intermédiaire du réseau de communication 120 (il peut alors le faire au cours de l'opération 412,

- soit choisir d'effacer des fichiers relatif à des pages mémorisées (il est alors invité à effectuer un effacement manuel (voir, par exemple, l'opération 517, figure 5B)

- soit autoriser une compression desdits fichiers avec un taux de compression supérieur à celui qui est utilisé pour les fichiers mémorisés (dans ce dernier cas, au cours de l'opération 412, les fichiers images et/ou les fichiers sons, des premières pages mémorisés sont décompressés puis recompressés avec un plus fort taux de compression, jusqu'à ce que l'espace mémoire alloué soit respecté).

A titre de deuxième exemple, non exclusif du premier exemple, les fichiers sont effacés en fonction de leur type, les fichiers images animés, images fixes, puis, sons, puis, graphiques, puis textes étant effacés au bout de durées différentes.

Par exemple, les fichiers images animées sont conservés deux fois moins longtemps que les fichiers images fixe qui sont conservés deux fois moins longtemps que les fichiers sons, qui sont conservés deux fois moins longtemps que les fichiers graphiques qui sont conservés deux fois moins longtemps que les fichiers textes qui sont conservés deux fois moins longtemps que les liens entre les pages qui sont conservés deux fois moins longtemps que les adresses des pages.

A titre de troisième exemple, non exclusif des deux premiers, les informations relatives aux pages les plus anciennement mémorisées sont effacées en premier.

A titre de quatrième exemple, non exclusif des trois premiers, les informations relatives aux différents sujets sont conservés pendant des durées différentes.

A titre de cinquième exemple, non exclusif des quatre premiers, les informations relatives au pages d'un site avec lequel une transaction a été effectuée sont conservés plus longtemps que les autres, et, par exemple, pendant au moins une durée égale à une garantie légale plus un délai de livraison maximal (par exemple, si le délai de garantie est de 12 mois, la durée de conservation des informations sera d'au moins 15 mois).

A la suite de l'opération 412, l'opération 409 est réitérée.

Les figures 5A et 5B représentent un organigramme de mise en oeuvre du sixième aspect de la présente invention. A la suite d'une mise en fonctionnement du logiciel

d'assistance, soit automatiquement à la mise en fonctionnement du terminal 100, soit par sélection d'un icône spécifique (non représenté) au cours de l'opération 500, au cours de l'opération 501, l'utilisateur peut sélectionner une fonction de relecture des pages reçues au cours de communications sur un réseau de communication et mémorisées sur le disque dur 102.

Au cours d'une opération 502, l'utilisateur sélectionne une fonction liée à la relecture, par exemple en utilisant des icônes illustrés en figure 6.

Au cours du test 503, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'ordonner les pages mémorisées par sujet, ou non. Lorsque le résultat du test 503 est positif, au cours d'une opération 504, l'unité centrale 106 affiche une liste des sujets existants et, lorsque l'utilisateur a choisi un sujet, ordonnance les informations conservées en mémoire en relation avec le sujet sélectionné, date par date, en ordre inverse de l'ordre chronologique. A la suite de l'opération 504, l'opération 502 est réitérée.

Lorsque le test 503 est négatif, au cours d'un test 505, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'ordonner les pages mémorisées par date, ou non. Lorsque le résultat du test 505 est positif, au cours d'une opération 506, l'unité centrale 106 ordonnance les informations conservées en mémoire, date par date, en ordre inverse de l'ordre chronologique. A la suite de l'opération 506, l'opération 502 est réitérée.

Lorsque le test 505 est négatif, au cours d'un test 507, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'effectuer une relecture rapide des pages mémorisées, ou non. Lorsque le résultat du test 507 est positif, au cours d'une opération 508, l'unité centrale 106 affiche des premières portions de page, et chaque page pendant une première durée prédéterminé, dans l'ordre défini par ordonnancement, ou, à défaut, data par date, dans l'ordre chronologique. Les premières portions de page comportent préférentiellement, au moins, l'adresse de la page et, préférentiellement, la partie haute de la page comportant au moins les textes de cette partie haute de la page. Lorsque l'opération 508 est lancée, l'opération 502 peut être réitérée.

Lorsque le test 507 est négatif, au cours d'un test 509, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'effectuer une relecture lentes des pages mémorisées, ou non. Lorsque le résultat du test 509 est positif, au cours d'une opération 510, l'unité centrale 106 affiche des deuxièmes portions de page, et chaque page pendant une deuxième durée prédéterminé plus longue que la première durée prédéterminée, dans l'ordre défini par ordonnancement, ou, à défaut, les fichiers dotés d'une interdiction d'effacement

automatique (voir opération 519) avant les autres et, dans chaque groupe, data par date, dans l'ordre chronologique. Les deuxièmes portions de page comportent, préférentiellement, au moins les premières portions. Les deuxièmes portions peuvent comporter les textes de toute la page, avec défilement de la page, de haut en bas, pour afficher ces textes. Ils peuvent, aussi comporter les graphiques, les images fixes, les sons et les images animée. Lorsque l'opération 510 est lancée, l'opération 502 peut être réitérée.

Lorsque le test 509 est négatif, au cours d'un test 511, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'arrêter la relecture, ou non. Lorsque le résultat du test 511 est positif, au cours d'une opération 512, l'unité centrale 106 arrête le défilement sur la page en cours et provoque l'affichage et la diffusion du contenu de chaque fichier associé à ladite page, y compris les fichiers sons et images animées. A la suite de l'opération 512, l'opération 502 est réitérée.

Lorsque le test 511 est négatif, au cours d'un test 513, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'effectuer une relecture lente en sens inverse, ou non. Lorsque le résultat du test 513 est positif, les mêmes opérations qu'au cours de l'opération 510 sont effectuées mais dans l'ordre inverse. Lorsque l'opération 514 est lancée, l'opération 502 peut être réitérée.

Lorsque le test 513 est négatif, au cours d'un test 515, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'effectuer une relecture rapide en sens inverse, ou non. Lorsque le résultat du test 515 est positif, les mêmes opérations qu'au cours de l'opération 508 sont effectuées mais dans l'ordre inverse. Lorsque l'opération 516 est lancée, l'opération 502 peut être réitérée.

Lorsque le test 515 est négatif, au cours d'un test 517, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'effacer des informations, ou non. Lorsque le résultat du test 517 est positif, la page en cours d'affichage reste affichée pendant toute l'opération 518. Une liste des fichiers attachés à la page en cours d'affichage est affichée dans une fenêtre en surimpression sur la page en cours d'affichage et l'utilisateur sélectionne les fichiers qu'il souhaite effacer. Ces fichiers sont alors effacés du disque dur 102. Lorsque l'effacement est opéré, la fonction précédemment sélectionnée avant celle d'effacement est reprise et l'opération 502 peut être réitérée.

Lorsque le test 517 est négatif, au cours d'un test 519, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est d'affecter la page en cours d'affichage d'une interdiction d'effacement automatique, ou non. Lorsque le résultat du test 519 est

positif, au cours d'une opération 520, l'adresse de la page en cours d'affichage est associée à un drapeau qui indique que les fichiers relatifs à cette page ne peuvent être effacés automatiquement, par exemple au cours d'une opération de gestion de mémoire automatique. Lorsque l'opération 520 est effectuée, l'opération 502 peut être réitérée.

Lorsque le test 519 est négatif, au cours d'un test 521, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est de changer le sujet de référence de la page la page en cours d'affichage, ou non. Lorsque le résultat du test 521 est positif, au cours d'une opération 522, la page en cours d'affichage reste affichée pendant toute la durée de l'opération 522 et, dans une fenêtre superposée à la page en cours d'affichage, les différents sujets référencés ainsi qu'une option de création d'un nouveau sujet sont proposés à l'utilisateur. L'utilisateur sélectionne alors le nouveau sujet auquel la page en cours d'affichage doit être lié et le sujet associé à la page est modifié en mémoire sur le disque dur 102. Lorsque l'opération 522 est effectuée, l'opération 502 peut être réitérée.

Lorsque le test 521 est négatif, au cours d'un test 523, l'unité centrale 106 détermine si la fonction sélectionnée au cours de l'opération 502 est de sortir de la fonction de relecture. Lorsque le résultat du test 523 est positif, la fonction de relecture est arrêtée et une fenêtre de dialogue affichée sur l'écran de visualisation 104 permet à l'utilisateur de sélectionner d'autres fonctions. Lorsque le résultat du test 523 est négatif, l'opération en cours de poursuit, s'il s'agit de l'une des opérations 508, 510, 514 ou 516 et l'opération 502 peut être réitérée.

La figure 6 représente un écran de visualisation 600 au cours d'une opération de relecture de l'organigramme illustré en figure 5. Cet écran 600 correspond, par exemple, à ce qui est affiché par l'écran de visualisation 104 au cours de l'une des opérations 508, 510, 514 et 516, lorsque l'opération 502 peut être réitérée.

Dans l'écran 600, un zone principale 620 représente une partie d'une page relue en mémoire dans le disque dur 102. Une zone graphique 610 représente des pages conservées en mémoire dans le disque dur 102 et leurs liens. Ici les pages reçues à la date du 11/06/99, au cours d'une session de communication entamée à 11 heures et 5 minutes sont représentées dans la partie supérieure de la zone graphique 610 et les premières pages reçues le 11/06/99, au cours d'une session de communication entamée à 17 heures et dix minutes, sont représentées dans la partie basse de zone graphique 610. Chaque page est représentée dans la zone graphique 610 sous forme d'un cercle et deux cercles qui se touchent et dont les centres sont reliés par une ligne droite pleine correspondent à deux pages qui ont été visitées successivement.

Par exemple, une succession de cercles 1 à 5 représentée comme suit

1

2 3 4

5

où les cercles 1 et 2, 2 et 3, 3 et 4 et 3 et 5 se touchent respectivement deux à deux et dont les centres sont reliés par une ligne droite pleine, deux à deux, indiquent que l'utilisateur a visité successivement les pages 1, 2, 3, 4, 3 et 5. Si un lien est indiqué par une ligne droite entre deux cercles qui ne se touchent pas, cela indique que les deux pages représentées possèdent une adresse identiques.

Le cercle noir indique la page en cours de visualisation. Les liens tracés en traits interrompus concerne les pages qui sont représentées dans deux sessions de communication différentes, c'est-à-dire qui ont été reçues au cours de deux sessions différentes. Lorsque l'un de ces traits (plein ou interrompu) comporte une flèche, cela indique que la page a été reçue avec plus d'information au cours de l'occurrence indiquée par la pointe de la flèche qu'au cours de chaque autre occurrence.

La zone de sélection de fonction basse 630 comporte des formes géométriques, dont certaines sont bien connues des utilisateurs de magnétoscope ou de magnétophone et des informations écrites.

Le rectangle le plus à gauche, référencé 641, indique le sujet en cours de relecture, ici « appareils photos ». les rectangles 642 et 643 indiquent qu'il y a deux autres sujets que l'utilisateur peut choisir. Le double triangle orienté à gauche 631 correspond à la relecture rapide en sens inverse de l'ordonnancement sélectionné et permet de sélectionner l'opération 516. Le triangle orienté à gauche 632 correspond à la relecture lente en sens inverse de l'ordonnancement sélectionné et permet de sélection l'opération 514. Le carré 633 correspond à l'arrêt de relecture et permet de sélectionner l'opération 512. Le triangle orienté à droite 634 correspond à la relecture lente dans l'ordre de l'ordonnancement sélectionné et permet de sélection l'opération 510. Le double triangle orienté à droite 635 correspond à la relecture rapide dans l'ordre de l'ordonnancement sélectionné et permet de sélectionner l'opération 508.

Le mot « effac » 636 permet à l'utilisateur de provoquer l'opération 518. Le mot « impor » 637 permet à l'utilisateur de provoquer l'opération 520. Le mot « out » 638 permet à l'utilisateur de provoquer la sortie de la fonction de relecture. Le mot « chang » 639 permet à l'utilisateur de sélectionner l'opération 522.

On observe que l'utilisateur peut sélectionner la prochaine page à afficher directement sur le plan affiché dans la zone 610, par utilisation de la souris 103.

D'une manière générale, selon le troisième aspect de la présente invention, au cours d'une session de communication entre le terminal 100 et un site 150, une deuxième session de communication est ouverte entre le terminal 100 et un site de protection 170 et une information relative au site 150 est transmise automatiquement au site de protection 170. Préférentiellement, n retour, une information relative à la première session de communication est transmise automatiquement au terminal 100 par le site de protection 170.

La figure 7 représente un organigramme de mise en oeuvre du troisième aspect du procédé visé par la présente invention.

Au cours d'une opération 702, le site 150 et au cours d'une opération 704, le terminal 100 ouvrent une session de communication entre eux. Au cours d'une opération 706, le site 150 et au cours d'une opération 708, le terminal 100 initient une communication d'information protégée, et, dans le cas illustré en figure 7, une transaction nécessitant un paiement en ligne par transmission d'un identificateur d'un moyen de paiement.

Au cours d'une opération 710, le terminal 100 et au cours d'une opération 712, le tiers de protection ou d'assistance 170 ouvrent une deuxième session de communication. Au cours d'une opération 714, le terminal 100 transmet au site de protection 170 un identifiant du site 150, par exemple sous la forme d'un identifiant de la page en cours d'affichage, et plus particulièrement l'adresse de ladite page. Au cours d'une opération 716, le site de protection reçoit ledit identifiant.

Au cours d'une opération 718 le tiers de protection transmet au terminal 100 des informations relatives à la première session. Par exemple :

- le pays d'implantation du site 150,
- le droit applicable à la communication de l'information protégée, identifié par le pays de résidence du site 150,
- la durée de garantie légale d'un achat auprès du site 150,
- un taux de risque de transaction frauduleuse avec le site 150, évalué à partir de statistiques par exemple disponibles auprès d'un site tel que « fraud.org »,
- un taux de satisfaction d'autres clients du site 150, évalué à partir d'informations transmises par les clients ou par un site tel que « bizrate.com »,
- une publicité relative aux produits promus par le site 150,

- une offre de mise en relation avec des sites concurrents du site 150,

- une offre de détection automatique d'encryptage de la première session,

- une date d'établissement du site 150, obtenue auprès du site « internic.com »,

- une offre de conseils relatifs à la transaction en cours,

- une certification d'informations provenant du site 150,

- une certification du site 150, par exemple telle qu'effectuée par le site « verisign.com », éventuellement complétée des opérations recommandées par ce site,

- une date certifiée de la première session destinée à être combinée à des informations à mémoriser,

- un identificateur de moyen de paiement de substitution pour protéger le moyen de paiement habituel de l'utilisateur,

sont des informations relatives à la première session.

Préférentiellement, les informations relatives à la première session qui sont transmises par le site de protection 170 comporte des informations relatives au site 150 et/ou aux caractéristiques techniques de la première session.

Cependant, complémentairement, des informations telles que :

- une offre de mise en relation avec un moteur de recherche de meilleurs prix,

- un questionnaire à remplir, dont les réponses sont destinées à être conservées en mémoire,

- des conseils de prudence généraux, par exemple inspirés des conseils offerts par le site « fraud.org »,

peuvent être transmises par le tiers de protection 170.

Le terminal 100 reçoit et traite ces informations au cours d'une opération 720.

En figure 7, on a représenté le cas où l'utilisateur choisit de visiter un autre site, dit « tiers marchand » concurrent du site 150, par exemple en fonction du résultat d'une recherche effectuée par un moteur de recherche de meilleur prix.

Au cours de l'opération 722, le terminal 100 et, au cours de l'opération 724, le site tiers marchand ouvrent une troisième session de communication. Au cours de l'opération 726, le terminal 100 et, au cours de l'opération 728, le site tiers marchand initient une communication d'information protégée, et, dans le cas illustré en figure 7, une transaction nécessitant un paiement en ligne par transmission d'un identificateur d'un moyen de paiement.

Au cours d'une opération 730, le terminal 100 et au cours d'une opération 732, le tiers de protection ou d'assistance 170 ouvrent une quatrième session de communication. Au cours d'une opération 734, le terminal 100 transmet au site de protection 170 un identifiant du site tiers marchand, par exemple sous la forme d'un identifiant de la page en cours d'affichage, et plus particulièrement l'adresse de ladite page. Au cours d'une opération 736, le site de protection reçoit ledit identifiant.

Au cours d'une opération 738 le tiers de protection transmet au terminal 100 des informations relatives à la troisième session. Au cours de l'opération 740, le terminal 100 reçoit et traite lesdites informations relatives à la troisième session.

A titres d'exemple, en figure 7, on a représenté un grand nombre d'échanges d'informations entre le terminal 100 et le site de protection 170, au cours des opérations 738 à 764. Cependant, conformément au troisième aspect de la présente invention, au moins une information relative à la troisième session est transmise au cours de l'opération 738.

Dans l'exemple illustré en figure 7, complémentairement à la transmission d'information relative à la troisième session effectuée par le site de protection 170 au terminal 100 au cours de l'opération 738, au cours d'une opération 742 le terminal 100 requiert la transmission de taux de risque et de satisfaction. Le site de protection 170 reçoit cette requête au cours de l'opération 744 et transmet ces taux au cours de l'opération 746. Le terminal 100 reçoit ces taux et les affiche à l'utilisateur au cours d'une opération 748.

Comme indiqué plus haut, chacun de ces taux peut être basé sur des statistiques de fraude et de satisfaction officielles (par exemple pays par pays ou état par état, par moyen de paiement utilisé, par type de transaction en cours, par site ...) ou disponibles sur un réseau tel que le réseau Internet, et/ou sur des informations fournies par des visiteurs du site de protection 170 (voir la figure 16).

Au cours d'une opération 750 le terminal 100 requiert la transmission d'un questionnaire légal. Le site de protection 170 reçoit cette requête au cours de l'opération 752 et transmet ce questionnaire au cours de l'opération 754. Le terminal 100 reçoit ce questionnaire et l'affiche à l'utilisateur au cours d'une opération 756. Le questionnaire peut comporter des questions auxquelles il faut répondre soit automatiquement, par la mise en oeuvre du logiciel d'assistance, soit manuellement, par saisie au clavier 105 en vue d'une conservation de trace légale de la transaction. Par exemple, ces informations peuvent comporter un identifiant du site 170, un identifiant de l'utilisateur, une date de transaction, un objet de la transaction et un montant de transaction. Le questionnaire peut aussi comporter des

question dont les réponses sont optionnelles mais qui servent à mettre en garde l'utilisateur sur les conséquences de la transaction ou sur la méconnaissance qu'il a du site tiers marchand.

Le terminal 100 transmet les réponses au questionnaire, et, éventuellement, des pages attachées qui proviennent de la troisième session, au site de protection 170 avec une requête de séquestre, au cours d'une opération 758. Le site de protection 170 reçoit ces informations au cours d'une opération 760 et les encrypte en y ajoutant une date certifiée et un certificat d'intégrité, et les renvoie au terminal 100, au cours d'une opération 762. Le terminal 100 reçoit ces informations cryptées et le certificat d'intégrité au cours d'une opération 764 et les place en mémoire dans le disque dur 102, et, le cas échéant, en les dotant d'une interdiction d'effacement automatique (voir opération 519). En variante, le site de protection 170 stocke une double de ces informations ou le certificat d'intégrité qui permet de détecté si les informations conservées en mémoire sont modifiées ultérieurement.

Au cours de l'opération 766, le terminal 100 transmet une requête de moyen de paiement à usage unique auprès d'un site financier proposé par le site de protection 170. Le site financier reçoit cette requête au cours d'une opération 768.

Le site financier fournit, au cours d'une opération 770, au terminal 100, une information destinée à participer à la détermination d'un identificateur d'un moyen de paiement à usage unique.

Par exemple l'identificateur d'une carte de paiement à usage unique est constitué des huit premiers chiffres d'une carte de paiement réelle et de huit chiffres fournis par le site financier. On observe que la date de péremption de ladite carte peut faire partie des informations fournies par le site financier et correspondre à un code.

Selon une autre variante, le logiciel d'assistance implanté sur le terminal 100 permet un codage du numéro de carte de paiement de l'utilisateur, par l'intermédiaire d'une clé fournie par le site financier, de telle manière que le numéro codé soit ultérieurement décodé par un organisme financier, par exemple le même site financier et permette d'effectuer un paiement.

Lorsque l'utilisateur est déjà référencé auprès du site financier, c'est-à-dire qu'un numéro de compte permanent lui est attribué, le site financier effectue préalablement une authentification de l'utilisateur. Puis le site tiers financier ne transmet pas de numéro de carte de paiement intégral, pour éviter que ce numéro puisse être piraté, c'est-à-dire utilisé par un tiers. Au contraire, préférentiellement, le site financier fourni une racine qui permettent la détermination d'un identificateur de moyen paiement par l'utilisateur ou le terminal 100 mais

ne permettent pas de constituer, avec la racine seule, un identificateur de moyen de paiement. Cette caractéristique est opposée au mode de fonctionnement décrit dans le brevet U.S. 5,883,810 qui est intégralement incorporée ici par référence. La racine fournie par le site financier et/ou la détermination de l'identificateur du moyen de paiement à usage unique dépendent, préférentiellement, d'identificateurs de la transaction financière, comme son montant, l'identificateur de son bénéficiaire et/ou l'identificateur du site financier.

La racine fournie par le site financier peut être générée comme un certificat de transaction de la transaction en cours.

Le terminal 100 reçoit l'information destinée à participer à la détermination d'un identificateur de moyen de paiement à usage unique au cours de l'opération 772. Il détermine l'identificateur de moyen de paiement à usage unique au cours de l'opération 774, par exemple en mettant en oeuvre une fonction de calcul à sens unique du logiciel d'assistance, agissant sur l'information reçue de la part du site financier, d'un numéro de carte de paiement, d'un identificateur du site 150 et d'un montant de transaction. Eventuellement, un certification de transaction est aussi utilisé pour la détermination de l'identificateur de moyen de paiement à usage unique.

Dans l'exemple illustré en figure 7, au cours de l'opération 776, le terminal 100 et, au cours de l'opération 778, un site tiers de confiance 180 ouvrent une cinquième session de communication. Au cours d'une opération 780, le terminal 100 transmet des informations à séquestrer au site tiers de confiance. Ces informations sont des informations légales liées à la transaction effectuée avec le site tiers marchand. Au cours de l'opération 782, le site tiers de confiance 180 met en mémoire ces informations, éventuellement cryptées et dotées d'un certificat d'intégrité.

Dans l'exemple illustré en figure 7, au cours d'une opération 784, le site de protection 170 transmet un message de sécurisation au site tiers marchand pour confirmer que la transaction a été sécurisée.

On observe que en figure 7, les sites de protection 170, site financier et site tiers de confiance 180 ont été représentés comme des entités indépendantes. Cependant, dans d'autres modes de réalisation du procédé de la présente invention, deux ou trois de ces sites sont confondus en une seule entité.

On observe que le site dit financier peut ne servir que d'intermédiaire entre les parties à la transaction (l'utilisateur et le site tiers marchand) et faire effectuer le paiement par un autre organisme financier, après lui avoir fourni un identifiant de l'utilisateur ou d'un moyen

de paiement réelle ou virtuel. En particulier, le site dit financier peut utiliser la racine qu'il a transmise et, éventuellement, des informations qu'il a reçu de la part du terminal 100, pour déterminer un numéro de carte de paiement permanent.

Par exemple si la clé transmise est une série de chiffres qui doivent être additionnés aux chiffres du numéro d'une carte de paiement permanente pour fournir, modulo 10, les chiffres de l'identificateur de moyen de paiement à usage unique, la clé conservée par le site financier peut lui servir à déterminer le numéro de la carte de paiement permanente.

On observe que, préférentiellement, toutes les communications mises en oeuvre conformément à la présente invention sont protégées par cryptage, selon des techniques connues ou à venir.

La figure 8 représente des fonctions mises en oeuvre dans différents systèmes informatiques reliés à un réseau de communication au cours d'un premier exemple de succession d'opérations mises en oeuvre conformément au quatrième aspect du procédé visé par la présente invention, dans le cas où l'utilisateur est référencé auprès du site financier. On observe en figure 8, qu'au cours d'une opération 800, le terminal 100 est connecté au site financier et qu'une session de communication est mise en place. Au cours d'une opération 801, le site financier et le terminal 100 organisent l'encryptage de la communication. Ensuite, au cours d'une opération 802, le site financier authentifie l'utilisateur du terminal 100 de manière connue, par exemple en lui demandant un code d'accès confidentiel et en vérifiant ce code.

Ensuite, au cours d'une opération 803, le site financier effectue une détermination de racine d'identificateur de moyen de paiement à usage unique. Cette racine est préférentiellement liée à un identificateur de l'utilisateur et conservé avec cet identificateur dans une mémoire (non représentée) du site financier. Par exemple, cette racine représente les huit derniers chiffres d'un numéro de carte de paiement à fournir à un site marchand tel que le site marchand 150 ou le site tiers marchand. Selon d'autres modes de réalisation, la racine est une clé de codage utilisée par un logiciel résident dans le terminal 100 pour générer un identificateur de moyen de paiement. Au cours d'une opération 804, la racine est fournie au terminal 100. Au cours d'une opération 805, la racine est validée en mémoire du site financier, dans une liste de racines valides. Selon une variante, le site financier détermine l'identificateur de moyen de paiement à usage unique que le terminal 100 va utiliser. Par exemple, le site financier connaît les huit premiers numéros d'une carte de paiement et y ajoute les huit derniers numéros qu'il fournit au terminal 100 ou la fonction de codage et les

racines utilisées par le terminal 100. Cet identificateur est alors conservé dans une mémoire d'identificateurs valides.

La session de communication avec le terminal 100 est alors interrompue. Lorsque le site marchant veut être payé, il fournit un identificateur de moyen de paiement au site financier. Au cours d'un test 806, le site financier détermine s'il a reçu un identificateur de moyen de paiement, ou non. Lorsque le résultat du test 806 est négatif, le test 806 est réitéré. Lorsque le résultat du test 806 est positif, au cours d'un test 807, le site financier détermine si l'identificateur de moyen de paiement est valide, ou non. A cet effet, par exemple, le site financier extrait la racine qu'il a fournit et la compare aux racines conservées dans la liste des racines valides. Selon un autre exemple, le site financier compare l'identificateur qu'il reçoit aux éléments d'une liste d'identificateurs valides qu'il a déterminé.

Lorsque le résultat du test 807 est positif, au cours d'une opération 808, le paiement est effectué. Lorsque le résultat du test 807 est négatif ou que l'opération de paiement 808 est achevée, au cours d'une opération 809, la racine de l'identificateur ou l'identificateur lui-même est invalidé dans la mémoire du site financier de telle manière que cette racine ou cet identificateur ne puisse être utilisé pour un paiement.

En variante, l'utilisateur fournit, au cours de l'opération 803, des informations relatives à la transaction, comme, par exemple, le nom de la société qui gère le site marchand (fournit, par exemple, par le tiers de protection 170) ou le montant de la transaction et l'identificateur du moyen de paiement à usage unique est déterminé de manière à être représentatif de ces informations ou à être associé, en mémoire du site financier à cet identificateur. De cette manière, la transaction peut être authentifiée par le site financier, au cours de l'opération 807, préliminairement au paiement, au cours de l'opération 808.

La figure 9 représente des fonctions mises en oeuvre dans différents systèmes informatiques reliés à un réseau de communication au cours d'un deuxième exemple de succession d'opérations mises en oeuvre conformément au quatrième aspect du procédé visé par la présente invention, dans le cas où l'utilisateur n'est pas référencé auprès du site financier. On observe en figure 9, que les opérations 901 à 903, 905 à 909 et 911 correspondent respectivement aux opérations 800 à 807 et 809.

A la suite de l'opération 903 et avant l'opération 905, au cours d'une opération 904, le terminal 100 fournit au site financier un identificateur de moyen de paiement permanent, tel qu'un numéro de carte de paiement.

A la suite du test 909, lorsqu'il est positif, au cours d'une opération 910, le site financier utilise l'identificateur de moyen de paiement qu'il a reçu du terminal 100 au cours de l'opération 904 pour obtenir un paiement auprès de l'organisme financier qui a délivré le moyen de paiement permanent. Ce paiement est effectué soit au profit du site marchand qui a fourni l'identificateur de moyen de paiement à usage unique, soit au profit du site financier, qui, ensuite, effectue le paiement au profit du site marchand qui a fourni l'identificateur de moyen de paiement à usage unique.

La figure 17 représente des fonctions mises en oeuvre dans différents systèmes informatiques reliés à un réseau de communication au cours d'un troisième exemple de succession d'opérations mises en oeuvre conformément au quatrième aspect du procédé visé par la présente invention, dans le cas où l'utilisateur n'est pas référencé auprès du site financier. On observe en figure 17, que les opérations 1701, 1702 sont identiques aux opérations 901 et 902. A la suite de l'opération 1702, au cours de l'opération 1703, le site financier détermine une racine ou un code de calcul et, au cours de l'opération 1704, le site financier fournit cette racine ou ce code au terminal 100 pour que celui-ci détermine un identificateur de moyen de paiement à usage unique.

Ce code peut être prédéterminé, en étant par exemple, fixe pendant une durée prédéterminée, prendre aléatoirement une parmi plusieurs valeurs possibles, ou dépendre d'une information liée à la transaction, comme le nom, le numéro de téléphone ou l'adresse de l'utilisateur ou l'adresse du site commerçant sur le réseau de communication.

On observe que, préférentiellement, le code est mis en oeuvre dans le terminal 100 de telle manière qu'un identificateur de moyen de paiement permanent puise être déterminé en connaissant la racine ou code et l'identificateur de moyen de paiement à usage unique.

Une fois la session entre le site financier et le terminal 100 achevée, le terminal 100 utilise la racine ou code fournie par le site financier au cours de l'opération 1704 pour déterminer un identificateur de moyen de paiement selon des techniques numériques connues.

Lorsque, au cours d'une opération 1705, le site financier reçoit un identificateur de moyen de paiement, il reçoit aussi des informations liées à la transaction. Le site financier peut donc déterminer la racine ou le code générateur qu'il a fournit au cours de l'opération 1704, même si ce code dépend d'informations liées à la transaction.

Au cours d'un test 1706, le site financier détermine si ce code est valide et si le l'identificateur de moyen de paiement à usage permanent est valide. Si les deux sont valides, l'opération 1707 est effectuée. Sinon, l'opération 1708 est effectuée.

Les opérations 1707 et 1708 correspondent aux opérations 910 et 911.

Selon une variante non représentée, la date de péremption liée à l'identificateur de moyen de paiement à usage unique permet d'identifier un code générateur ou un racine.

La figure 16 représente un organigramme de fonctionnement du dispositif illustré en figure 1, pour la mise en oeuvre du cinquième aspect de la présente invention. Cet aspect peut être combiné, ou non, à certaines des autres aspects de la présente invention.

Au cours d'une opération 1601, l'utilisateur du terminal 100 détermine une date à laquelle il considère qu'il serait satisfait d'avoir été fourni du produit ou service qu'il a payé sur le réseau de communication 120.

Ensuite, l'unité centrale 106, mettant en oeuvre le logiciel d'assistance, effectue une surveillance de la survenance de la date sélectionnée, au cours d'une opération 1602, qui peut s'étendre, en tâche de fond sur plusieurs jours. Lorsque la date survient, au cours d'une opération 1603, l'unité centrale 106 provoque l'affichage, sur l'écran de visualisation 104, d'une fenêtre de dialogue demandant si le produit ou service a bien été fourni.

Que la réponse soit positive ou négative, une autre question demande à l'utilisateur le degré de satisfaction ou d'insatisfaction dans lequel il est concernant la fourniture du produit ou service fourni, au cours d'une opération 1604. En outre, lorsque la réponse est négative, une nouvelle date est demandée à l'utilisateur et le processus est renouvelé.

L'information de satisfaction et l'éventuelle nouvelle date sont mis en mémoire 102 par le terminal 100, au cours d'une opération 1605.

Lorsque, au cours d'une opération 1606, le terminal 100 se connecte au réseau 120, et quel que soit le site auquel se connecte le terminal, un message de satisfaction comportant l'identificateur du site marchand et le degré de satisfaction de l'utilisateur ainsi que le délai de livraison, est automatiquement transmis au site de protection 170 au cours d'une opération 1607. Ce message peut prendre la forme d'un courrier électronique (« e-mail ») ou toute autre forme reconnue par le site de protection 170.

Grâce à ce message, le site de protection 170 peut déterminer les sites marchands qu'il peut recommander à ses visiteurs.

La figure 10 représente ce qui est affiché par l'écran de visualisation 104 lorsque l'utilisateur du terminal 100 a sélectionné une offre commerciale de la part du site informatique distant 150 et que cet utilisateur s'apprête à effectuer un paiement en ligne, en fournissant des informations concernant une carte de paiement telles que le numéro et la date d'expiration de la carte de paiement.

De manière simplifiée, l'écran de visualisation 104 affiche alors :

- une portion principale 1000 qui représente une portion d'une page reçue en provenance du site informatique distant 150 ;

- une bandeau supérieur 1010 qui affiche, et permet de sélectionner, des fonctions ou des menus déroulants ;

- un bandeau inférieur 1050 qui affiche des informations générales et des zones de sélection de fonction et

- un bandeau latéral 1080 qui permet de faire défiler la page affichée dans la portion principale 1000.

Dans l'exemple illustré en figure 10, la portion principale 1000 comporte, au cours de la phase de la transaction qui correspond au début d'un paiement en ligne :

- une portion d'une page reçue en provenance du site informatique distant 150 comportant des informations textuelles d'une offre commerciale 1020, éventuellement des informations graphique ou d'image (non représentées) et est associée à une séquence sonore (non représentée) ;

- des informations de sélection 1030 d'au moins un autre page du site informatique distant 150 ;

- des conditions commerciales 1035 ;

- un icône mobile 1090 représentant la position sélectionnée par la souris 103 et

- une portion centrale de paiement en ligne 1040.

La portion centrale 1040 comporte, par exemple, des cases 1041 de sélection d'un type de carte de paiement, une zone d'écriture 1042 d'un numéro de carte de paiement, un zone d'écriture 1043 d'un mois d'expiration de la durée de validité de carte de paiement et une zone de validation 1044 de la saisie des informations relatives au paiement électronique en ligne et de la transaction.

Le bandeau supérieur 1010 affiche deux flèches latérales 1084 qui, lorsque l'une d'entre elles est sélectionnée par usage de la souris 103, permettent de retourner à la page précédemment affichée dans la portion centrale 1000 (flèche orientée à gauche) ou d'avancer à la page affichée à la suite de la page en cours d'affichage dans la portion centrale 1000 (flèche orientée vers la droite) selon des conventions connues dans les logiciels de navigation sur Internet. Le bandeau supérieur 1010 affiche aussi des en-têtes de menus déroulant bien connus dans les logiciels de navigation, tels que :

- « fichier », pour créer, ouvrir, sauvegarder, imprimer ou fermer un fichier,

- « édition », pour sélectionner, couper, copier, coller, des informations,

- « accès Internet », pour rechercher un site Internet ou s'y connecter à partir de son adresse,

- « messagerie » pour accéder à sa messagerie personnelle, et

- « sites favoris », pour accéder directement à des sites Internet préalablement sélectionnés comme sites favoris.

L'utilisation de la souris 103 permet de sélectionner l'une des fonctions ou l'un des menus déroulants illustrés (parfois sous forme d'icônes) dans le bandeau supérieur 1010.

Le bandeau latéral 1080 comporte :

- une flèche supérieure 1082 orientée vers le haut, dont la sélection provoque le défilement de la page illustrée dans la portion principale 1000, vers le haut, pour en afficher sa partie supérieure,

- une flèche inférieure 1083 orientée vers le bas, dont la sélection provoque le défilement de la page illustrée dans la portion principale 1000, vers le bas, pour en afficher sa partie inférieure,

- une portion 1081 qui, en combinaison avec une portion 1085, représente la proportion de la page illustrée dans la portion principale 1000 qui est affichée et

- une portion 1085 qui représente, avec la même facteur de proportionnalité que la portion 1081, la partie inférieure de la page illustrée dans la portion principale 1000 qui n'est pas visible.

Le bandeau inférieur 1050 affiche des informations générales, telles que le nom du fournisseur d'accès, la durée de la connexion au fournisseur d'accès déjà écoulée, le logiciel de navigation utilisé (par exemple de l'une des marques déposées Netscape, Microsoft ou AOL) et des zones de sélection de fonction. Ici deux zones de sélection de fonctions 1060 et 1070 déclenchent une sauvegarde d'au moins une information de contenu d'au moins les portions des pages du site informatique distant 150 qui ont été reçues de la part du site informatique distant 150 et affichées sur l'écran de visualisation 104.

La zone 1060 affiche, en clair, la fonction de sauvegarde sous la forme de deux mots « sauvegarde commerciale ». La zone 1070 affiche, sous forme d'un icône représentant une balance, symbole de la justice, la fonction de sauvegarde. Selon différentes variantes de la présente invention :

- seules les portions qui ont été affichées,

- seules des informations de contenu ou de contexte, comme le nom du fournisseur et la date de la transaction,

- seuls certains mots présents dans ou représentant ces portions ou le fichier sonore reçu et diffusé,

- seuls les textes présents dans ces pages,

- les textes et les images,

- les pages entières,

- le fichier sonore,

- les informations de déplacement effectués dans les pages en cours d'affichage, et/ou

- la durée d'affichage de chaque portion de la page sur l'écran de visualisation 104

sont mis en mémoire non volatile, par exemple la mémoire 102 par déclenchement de la fonction de sauvegarde liée aux deux zones de sélection de fonctions 1060 et 1070.

Cette fonction et/ou d'autres fonctions de sécurisation sont aussi déclenchées de manière automatique par détection de préparation d'un paiement par transmission d'un identifiant de moyen de paiement au cours de la session de communication avec le site informatique distant 150, par l'intermédiaire du terminal 100, comme exposé en regard de l'opération 307, en regard des figures 1, 1 et 12.

Selon un aspect de l'invention, et d'une manière générale, l'utilisateur met d'abord en fonctionnement un terminal informatique et accède, par l'intermédiaire d'un réseau de communication, à un site informatique distant.

Le terminal ouvre alors une session de communication avec le site informatique distant et reçoit, de la part du site informatique une offre de transaction. En tâche de fond, le terminal ou un système informatique par lequel transite des données échangées entre le terminal et le site informatique distant au cours de la session de communication, détermine si un paiement est préparé au cours de la session et par l'intermédiaire du terminal, par exemple en reconnaissant un identifiant d'une carte de paiement.

Si tel est le cas, le terminal ou le système informatique effectue une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur du terminal. Cette opération de sécurisation comporte, au moins une opération de sauvegarde du montant du paiement, par exemple, en effectuant au moins l'une des opérations suivantes:

- création d'un fichier de sauvegarde et mise en mémoire d'au moins une parties des données au format « texte » échangées au cours de la session de communication entre le terminal et le site informatique ;

- constitution d'un message crypté représentatif d'au moins le montant de la transaction et, préférentiellement, d'un identifiant du fournisseur et transmission de ce message à un tiers de confiance comme, par exemple, un site informatique d'une banque auprès de laquelle le paiement doit être effectué ; et

- impression d'une trace de la transaction, comportant, au moins la date, le montant de la transaction, et, préférentiellement, le nom du fournisseur et un code d'intégrité (et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus) ; et

- affichage d'un questionnaire que l'utilisateur complète, s'il le souhaite, pour garder trace de la transaction, et sauvegarde du contenu de ce questionnaire s'il a été au moins partiellement renseigné.

En outre, l'opération de sécurisation peut comporter l'une des opérations suivantes :

- authentification du payeur, par exemple par affichage d'une demande de code secret puis vérification du code secret ;

- affichage de données juridiques ;

- impression d'un détail des paiements déjà effectués en ligne avec la carte concernée.

- transmission au site informatique avec lequel la transaction est en cours, d'une information représentative de la sécurisation de la transaction, comme, par exemple, un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur.

Plus particulièrement, au cours d'un mode de fonctionnement du dispositif illustré en figure 1, l'utilisateur met en fonctionnement le terminal 100 et accède, par l'intermédiaire du modem 101 et du réseau 120, à un fournisseur d'accès à Internet 130.

Ensuite, l'utilisateur sélectionne, par l'intermédiaire du terminal 100, un site informatique distant 150, par exemple en pointant, avec la souris 103 :

- un identifiant d'un site dans le menu déroulant « sites favoris »,

- un lien avec un site sur le portail d'accès du fournisseur d'accès, ou

- le menu déroulant « accès Internet » et en saisissant une adresse de page Internet ou de site Internet, commençant, par exemple, par les lettres « http » ou « www ».

Le terminal 100 entre alors en communication et ouvre une session de communication avec le site informatique distant 150 sélectionné, et lui envoie une information de sécurisation

de transaction. Cette information est une séquence de symboles spécifique qui indique que toute communication et/ou transaction est sécurisé selon un mode de réalisation du procédé visé par la présente invention. Puis, le terminal 100 reçoit, de la part du site informatique distant 150, une page Internet, par exemple une page d'accueil. Le terminal 100 provoque l'affichage, au moins partiel, de la page reçue. L'utilisateur peut alors déplacer cette page de manière à en prendre connaissance, plus ou moins complètement.

Ensuite, l'unité centrale 106 détermine si la page reçue est déjà conservée dans le disque dur 102, ou non. Si non, l'unité centrale 106 provoque la mémorisation d'au moins une information d'adresse de la page reçue, et, éventuellement, une information de contenu, telle que l'ensemble des données reçues au format « texte » pour la page concernée, dans le disque dur 102. Ensuite ou si la page reçue est déjà conservée dans le disque dur 102, l'unité centrale 106 détermine si l'utilisateur a sélectionné une autre page, par exemple par sélection d'un lien avec un autre page, tel que le lien 230.

Si l'utilisateur a sélectionné une autre page, et que la page sélectionnée n'a pas déjà été reçue au cours de la même session de communication entre le terminal 110 et le site informatique distant 150, le fonctionnement du terminal 100 déjà exposé ci-dessus est reproduit mais chaque page précédemment reçues est, au moins en partie (par exemple l'adresse de la page et/ou les données « texte » de cette page), conservée en mémoire cache 108. Sinon, l'unité centrale 106 détermine si un nombre prédéterminé de chiffres (par exemple quatre chiffres) saisis successivement correspondent à une séquence de chiffres d'une carte de paiement conservée en mémoire.

On observe ici que, par exemple lors de l'installation du logiciel qui permet l'application représentée ici, les quatre premiers chiffres des cartes de paiement de l'utilisateur lui sont demandées et sont mis en mémoire 102. Ensuite, en tâche de fond, chaque séquence de quatre chiffres saisis au clavier est comparée aux quatre premiers chiffres des cartes de paiement conservée en mémoire non volatile 102.

Si aucune séquence n'est reconnue, l'unité centrale 106 détermine si un autre site a été sélectionné par l'utilisateur, par exemple comme exposé ci-dessus ou par sélection d'un lien entre le site en cours de visite et un nouveau site, dans la zone principale 200. Si tel est la cas, ce que le terminal 100 a effectué vis-à-vis du site en cours est reproduit vis-à-vis du nouveau site visité. Si aucun autre site n'a été sélectionné, l'affichage de la page est les opérations suivantes sont réitérées.

Lorsqu'une séquence correspondant, par exemple, aux quatre premiers chiffres d'un numéro de carte de paiement est reconnue, l'unité centrale 106 effectue une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur du terminal. Cette opération de sécurisation comporte, au moins une sauvegarde locale ou à distance du montant du paiement, par exemple, en effectuant au moins l'une des opérations exposées ci-dessous :

- l'unité centrale 106 provoque l'affichage d'une fenêtre sur l'écran 104, fenêtre comportant un questionnaire que l'utilisateur complète, s'il le souhaite, pour garder trace de la transaction, le questionnaire portant, par exemple, sur le fournisseur, sur l'objet ou le service fournis, sur le montant de la transaction, sur le délai de fourniture, sur la garantie, sur le délai de réclamation, sur les conditions de remboursement en cas d'insatisfaction (pour remplir ce questionnaire, l'utilisateur peut minimiser la dimension de la fenêtre d'affichage du questionnaire et explorer les pages du site informatique distant 150) ;

- l'unité centrale 106 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les données au format « texte » des portions de pages du site informatique distant 150 qui ont été transmises au cours de la session de communication avec le site informatique distant 150. De manière préférentielle, cette mise en mémoire est associée à la mise en mémoire de la date. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit, au cours d'une lecture ultérieure, que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier. Le lecteur pourra, par exemple, s'inspirer des technique de marquage dites « watermarking » pour mettre en oeuvre cette fonction de code d'intégrité ;

- l'unité centrale 106 constitue un message crypté représentatif au moins du montant de la transaction et, préférentiellement d'un identifiant du fournisseur et ce message est transmis à un tiers de confiance 180, par exemple, le site informatique de la banque auprès de laquelle le paiement doit être effectué ; et/ou

- l'unité centrale 106 provoque l'impression de la date, du nom du fournisseur et du montant de la transaction, avec un code d'intégrité, et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus.

En outre, l'unité centrale 106 peut effectuer l'une des opérations suivante :

- l'unité centrale 106 affiche une demande de code secret (par exemple un nombre d'identification personnel connu sous le nom de PIN (pour Personal Identification Number) pour vérifier que l'utilisateur qui a saisi la séquence correspondant aux quatre premiers

chiffres d'un numéro de carte de paiement est bien autorisé à utiliser cette carte, puis vérifie que ce code secret correspond à un code conservé en mémoire dans le disque dur 102 ;

- l'unité centrale 106 affiche une fenêtre comportant des données juridiques (voir figure 13) ; et

- l'unité centrale 106 effectue l'impression d'un détail des paiements déjà effectués en ligne avec la carte concernée.

L'unité centrale 106 envoie ensuite, au site informatique distant 150, une information représentative de la sécurisation de la transaction est envoyée au site informatique distant 150. Cette information est, par exemple, identique à l'information déjà transmise au début de la session de communication. En variante, cette information de sécurité est un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur. En variante, cette information est un double du questionnaire mentionné ci-dessus, y compris des réponses fournies par l'utilisateur, afin qu'un document électronique contractuel soit connu des deux parties. Ensuite l'unité centrale 106 détermine, comme ci-dessus, si un autre site a été sélectionné, ou non, et poursuit, comme ci-dessus, la séquence d'opération, en fonction du résultat de cette détermination. On observe que la fin de la session de communication, c'est à dire la déconnexion du site Internet et la déconnexion du fournisseur d'accès sont effectuées de manière connue, au cours de l'affichage de la dernière page reçue de la part du site informatique distant 150, et ne sont donc pas détaillées ici.

La figure 11 représente un organigramme mettant en oeuvre un mode de réalisation du procédé objet de la présente invention. Au cours d'une opération 1100, il est accédé à un fournisseur d'accès à Internet.

Au cours de l'opération 1101, un site informatique distant est sélectionné, par exemple par l'intermédiaire :

- d'un identifiant d'un site dans un menu déroulant,

- d'un lien avec un site sur le portail d'accès du fournisseur d'accès, ou

- d'une adresse de page Internet ou de site Internet, commençant, par exemple, par les lettres « http » ou « www ».

Une session de communication est alors mise en place avec ce site informatique distant, au cours d'une opération 1102, et une information de sécurisation de transaction est transmise au site informatique distant. Cette information est une séquence de symboles spécifique qui indique que toute communication et/ou transaction est sécurisé selon un mode

de réalisation du procédé visé par la présente invention. Au cours de l'opération 1103, il est reçu, de la part du site informatique distant 150, une page Internet qui, au cours de la première itération de la fonction 1103, est une page d'accueil. Au cours de l'opération 1104, un affichage, au moins partiel, de la page reçue au cours de l'opération 1103 est effectué.

Au cours d'un test 1105, il est déterminé si la page reçue est déjà mémorisée localement, ou non. Si le résultat du test 1105 est négatif, au cours d'une opération 1106, la mémorisation d'au moins une information d'adresse de la page reçue, et, éventuellement, d'une information de contenu, telle que l'ensemble des données reçues au format « texte » pour la page concernée, est effectuée. A la suite de l'opération 1106 ou lorsque le résultat du test 1105 est positif, au cours d'un test 1107, il est déterminé si l'utilisateur a sélectionné une autre page, par exemple par sélection d'un lien avec un autre page.

Lorsque le résultat du test 1107 est positif et que la page sélectionnée n'a pas déjà été reçue au cours d'une opération 1103, l'opération 1103 est réitérée mais chaque page précédemment reçues est, au moins en partie (par exemple l'adresse de la page et/ou les données « texte » de cette page), conservée localement. Lorsque le résultat du test 1107 est négatif, au cours d'un test 1108, il est déterminé si un nombre prédéterminé de chiffres (par exemple quatre chiffres) saisis successivement correspondent à une séquence de chiffres d'une carte de paiement.

Par exemple, avant la mise en oeuvre du mode de réalisation du procédé exposé ici, les quatre premiers chiffres des cartes de paiement de l'utilisateur lui sont demandées et sont conservées localement. Dans cet exemple, au cours de l'opération 1108, pour chaque saisie d'une séquence d'au moins quatre chiffres successifs, chaque séquence de quatre chiffres successifs de la séquence est comparé à la séquence de quatre chiffres conservée localement.

Lorsque le résultat du test 1108 est négatif, au cours d'un test 1109, il est déterminé si un autre site a été sélectionné, par exemple selon l'une des manières exposées en regard de l'opération 1102 ou par sélection d'un lien entre le site en cours de visite et un nouveau site, dans la page affichée, ou non. Lorsque le résultat du test 1109 est positif, l'opération 1102 est réitérée. Lorsque le résultat du test 1109 est négatif, l'opération 1104 est réitérée.

Lorsque le résultat du test 1108 est positif, au cours d'une opération 1110, une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur est effectuée en sauvegardant au moins le montant du paiement. Par exemple l'opération 1110 comporte au moins l'une des opérations de sécurisation exposées ci-dessus.

A la suite de l'opération 1110, au cours d'une opération 1111, une information représentative de la sécurisation de la transaction est envoyée au site informatique distant avec lequel la session a été ouverte au cours de l'opération 1102. Cette information est, par exemple, identique à l'information transmise au cours de l'opération 1101. En variante, cette information de sécurité est un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire qui effectue les paiements liés à la carte, paye le fournisseur. En variante, cette information est un double du questionnaire mentionné ci-dessus, y compris des réponses fournies par l'utilisateur, afin qu'un document électronique contractuel soit connu des deux parties. A la suite de l'opération 1111, le test 1109 est effectué. On observe que la déconnexion du site Internet et la déconnexion du fournisseur d'accès sont effectuées de manière connue au cours de l'opération 1104, et ne sont donc pas détaillées ici.

Lorsque le mode de réalisation du procédé illustré en figure 11 est mis en oeuvre par le mode de réalisation du dispositif illustré en figures 1 et 10, au cours d'une opération 1100, l'utilisateur met en fonctionnement le terminal 100 et accède, par l'intermédiaire du modem 101 et du réseau 120, au fournisseur d'accès à Internet 130.

Au cours de l'opération 1101, l'utilisateur sélectionne, par l'intermédiaire du terminal 100, un site informatique distant 150, par exemple en pointant, avec la souris 103 :

- un identifiant d'un site dans le menu déroulant « sites favoris »,
- un lien avec un site sur le portail d'accès du fournisseur d'accès, ou
- le menu déroulant « accès Internet » et en saisissant une adresse de page Internet ou de site Internet, commençant, par exemple, par les lettres « http » ou « www ».

Le terminal 100 entre alors en communication avec le site informatique distant 150 sélectionné, au cours de l'opération 1102, et lui envoie une information de sécurisation de transaction. Cette information est une séquence de symboles spécifique qui indique que toute communication et/ou transaction est sécurisé selon un mode de réalisation du procédé visé par la présente invention. Au cours de l'opération 1103, le terminal 100 reçoit, de la part du site informatique distant 150, une page Internet qui, au cours de la première itération de la fonction 1103, est une page d'accueil. Au cours de l'opération 1104, le terminal 100 provoque l'affichage, au moins partiel, de la page reçue au cours de l'opération 1103. Au cours de l'opération 1104, l'utilisateur peut déplacer cette page de manière à en prendre connaissance, plus ou moins complètement, par l'intermédiaire de la souris 103 et de l'une des flèches 1082 et 1083.

Au cours du test 1105, l'unité centrale 1106 détermine si la page reçue est déjà conservée dans le disque dur 102, ou non. Si le résultat du test 1105 est négatif, au cours d'une opération 1106, l'unité centrale 106 provoque la mémorisation d'au moins une information d'adresse de la page reçue, et, éventuellement, une information de contenu, telle que l'ensemble des données reçues au format « texte » pour la page concernée, dans le disque dur 102.

A la suite de l'opération 1106 ou lorsque le résultat du test 1105 est positif, au cours du test 1107, l'unité centrale 106 détermine si l'utilisateur a sélectionné une autre page, par exemple par sélection d'un lien avec un autre page, tel que le lien 230.

Lorsque le résultat du test 1107 est positif et que la page sélectionnée n'a pas déjà été reçue au cours d'une opération 1103, l'opération 1103 est réitérée mais chaque page précédemment reçues est, au moins en partie (par exemple l'adresse de la page et/ou les données « texte » de cette page), conservée en mémoire cache 108. Lorsque le résultat du test 1107 est négatif, au cours du test 1108, l'unité centrale 106 détermine si un nombre prédéterminé de chiffres (par exemple quatre chiffres) saisis successivement correspondent à une séquence de chiffres d'une carte de paiement.

Lorsque le résultat du test 1108 est négatif, au cours du test 1109, l'unité centrale 106 détermine si un autre site a été sélectionné par l'utilisateur, par exemple selon l'une des manières exposées en regard de l'opération 1102 ou par sélection d'un lien entre le site en cours de visite et un nouveau site, dans la zone principale 1000, ou non. Lorsque le résultat du test 1109 est positif, l'opération 1102 est réitérée. Lorsque le résultat du test 1109 est négatif, l'opération 1104 est réitérée.

Lorsque le résultat du test 1108 est positif, au cours de l'opération 1110, l'unité centrale 106 effectue une opération de sécurisation contre un usage abusif du consentement contractuel de l'utilisateur du terminal 100 en sauvegardant au moins le montant du paiement. Cette opération de sécurisation comporte, par exemple, au moins l'une des opérations exposées ci-dessus. Par exemple, l'opération 1110 comporte au moins l'une des opérations de protection suivantes:

- l'unité centrale 106 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les données au format « texte » des portions de pages du site informatique distant 150 qui ont été transmises depuis l'opération 1102 de connexion à ce site informatique distant 150. De manière préférentielle, cette mise en mémoire est associée à la mise en mémoire de la date. De manière préférentielle, au cours de l'opération 1109, un code

d'intégrité est inséré dans le fichier et garantit, au cours d'une lecture ultérieure, que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier. Le lecteur pourra, par exemple, s'inspirer des technique de marquage dites « watermarking » pour mettre en oeuvre cette fonction de code d'intégrité ;

- l'unité centrale 106 affiche une fenêtre comportant un questionnaire que l'utilisateur complète, s'il le souhaite, pour garder trace de la transaction, le questionnaire portant, par exemple, sur le fournisseur, sur l'objet ou le service fournis, sur le montant de la transaction, sur le délai de fourniture, sur la garantie, sur le délai de réclamation, sur les conditions de remboursement en cas d'insatisfaction (pour remplir ce questionnaire, l'utilisateur peut minimiser la dimension de la fenêtre d'affichage du questionnaire et explorer les pages du site informatique distant 150) ;

- l'unité centrale 106 constitue un message crypté représentatif au moins du montant de la transaction et, préférentiellement d'un identifiant du fournisseur et ce message est transmis à un tiers de confiance 180, par exemple, le site informatique de la banque auprès de laquelle le paiement doit être effectué ; et/ou

- l'unité centrale 106 provoque l'impression de la date, du nom du fournisseur et du montant de la transaction, avec un code d'intégrité, et, lorsqu'il est disponible, le questionnaire complété mentionné ci-dessus.

En outre, cette opération de sécurisation comporte l'une des opérations ci-dessous :

- l'unité centrale 106 affiche une demande de code secret (par exemple un nombre d'identification personnel connu sous le nom de PIN (pour Personal Identification Number) pour vérifier que l'utilisateur qui a saisi la séquence reconnue au cours du test 1108 est bien autorisée à le faire, puis vérifie que ce code secret correspond à un code conservé en mémoire dans le disque dur 102 ;

- l'unité centrale 106 affiche une fenêtre comportant des données juridiques (voir figure 13) ;

- l'unité centrale 106 effectue l'impression d'un détail des paiements déjà effectués en ligne avec la carte concernée.

A la suite de l'opération 1110, au cours d'une opération 1111, une information représentative de la sécurisation de la transaction est envoyée au site informatique distant 150. Cette information est, par exemple, identique à l'information transmise au cours de l'opération 1101. En variante, cette information de sécurité est un certificat de transaction à usage unique qui doit être associée à la demande de paiement pour que l'organisme bancaire

qui effectue les paiements liés à la carte, paye le fournisseur. En variante, cette information est un double du questionnaire mentionné ci-dessus, y compris des réponses fournies par l'utilisateur, afin qu'un document électronique contractuel soit connu des deux parties. A la suite de l'opération 1111, le test 1109 est effectué. On observe que la déconnexion du site Internet et la déconnexion du fournisseur d'accès sont effectuées de manière connue au cours de l'opération 1104, et ne sont donc pas détaillées ici.

Selon une variante non représentée, le test 1108 et les opérations 1109 et 1110 sont effectuées par un système informatique par lequel transite les données échangées au cours de la session de communication ou les données envoyées par le terminal 100 au site informatique distant 150. Par exemple, le système informatique du fournisseur d'accès à Internet 130 peut effectuer ce test 1108 et ces opérations 1109 et 1110 pour le compte de ses clients.

Selon un autre aspect du procédé visé par la présente invention, l'opération de sécurisation comporte :

- une connexion à un site tiers,
- une fourniture au site tiers d'un identifiant du site avec lequel la transaction est en cours (par exemple son adresse Internet), un identifiant de l'utilisateur (par exemple son adresse Internet), et un montant du paiement,
- une fourniture, par le site tiers, d'une information codée qui est représentative de la date et, préférentiellement, d'au moins un des identifiants indiqués ci-dessus selon une fonction de codage confidentielle,
- une création d'un fichier de sauvegarde conservant au moins les portions en mode « texte » des portions de pages transmises par le site informatique distant avec lequel la transaction est en cours, ainsi que l'information codée reçue de la part du site tiers. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier,
- une fourniture, par le site tiers, d'informations relatives à la loi applicable à la transaction commerciale en cours, et des informations légales minimales concernant cette loi, par exemple la durée de garantie légale et le délai légal de réclamation auprès du fournisseur, et
- un affichage d'informations légales.

Selon une variante, au moins une partie de l'identifiant d'un moyen de paiement, par exemple des chiffres de la carte de paiement ou une règle prédéterminée respectée par cette

partie de l'identifiant, par exemple une somme des chiffres, sont transmises au site tiers de protection 170 et servent à calculer l'information codée.

Préférentiellement, la communication avec le site tiers de protection 170 est cryptée ou sécurisée, selon des techniques connues.

Selon un autre aspect de la présente invention, le dispositif illustré en figure 1 et, plus particulièrement l'unité centrale 106 mettent en oeuvre les opérations exposées ci-dessus, si ce n'est que l'unité centrale 106 effectue une opération de sécurisation au cours de laquelle :

- le terminal 100 se connecte, par l'intermédiaire du réseau 140, au site tiers de protection 170,

- le terminal 100 fournit au site tiers de protection 170 un identifiant du site informatique distant 150 (par exemple son adresse Internet), un identifiant de l'utilisateur (par exemple son adresse Internet), un montant de transaction,

- le site tiers de protection 170 fournit une information codée qui est représentative de la date et, préférentiellement, d'au moins un des identifiants indiqués ci-dessus selon une fonction de codage confidentielle,

- le terminal 100 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les parties textuelles des portions de pages du site informatique distant 150 qui ont été transmises depuis l'opération 302, ainsi que l'information codée reçue de la part du site tiers de protection 170. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier,

- le site tiers de protection 170 fournit au terminal 100 des informations relatives à la loi applicable à la transaction commerciale en cours, et des informations légales minimales concernant cette loi, par exemple la durée de garantie légale et le délai légal de réclamation auprès du fournisseur, et

- le terminal 100 provoque l'affichage d'informations légales (voir figure 13).

Selon une variante, au moins une partie d'un identifiant de moyen de paiement, ou une relation qu'elle respecte, par exemple le résultat de la somme de chiffres, est transmise au site tiers de protection 170 et sert à calculer l'information codée.

Préférentiellement, la communication entre le terminal 100 et le site tiers de protection 170 est cryptée ou sécurisée, selon des techniques connues.

La figure 12 représente un organigramme d'opérations et tests d'un deuxième mode de réalisation du procédé objet de la présente invention. Cet organigramme comporte les

fonctions et tests 1101 à 1104 et 1107 à 1109 de l'organigramme illustré en figure 11. Cependant, en comparaison avec l'organigramme illustré en figure 11, les opérations 1110 et 1111 sont remplacées par une opération 1209, au cours de laquelle :

- le terminal 100 se connecte, par l'intermédiaire du réseau 140, au site tiers de protection 170 ;

- le terminal 100 fournit au site tiers de protection 170 un identifiant du site informatique distant 150 (par exemple son adresse Internet), un identifiant de l'utilisateur (par exemple son adresse Internet), et un montant du paiement ;

- le site tiers de protection 170 fournit une information codée qui est représentative de la date et, préférentiellement, des identifiants indiqués ci-dessus selon une fonction de codage confidentielle ;

- le terminal 100 crée un fichier de sauvegarde dans la mémoire non volatile 102, et y enregistre au moins les parties textuelles des portions de pages du site informatique distant 150 qui ont été transmises depuis l'opération 1102, ainsi que l'information codée reçue de la part du site tiers de protection 170. De manière préférentielle, au cours de l'opération 1109, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier ;

- le site tiers de protection 170 fournit au terminal 100 des informations relatives à la loi applicable à la transaction commerciale en cours, et des informations légales minimales concernant cette loi, par exemple la durée de garantie légale et le délai légal de réclamation auprès du fournisseur et

- le terminal 100 provoque l'affichage d'informations légales (voir figure 13).

Selon une variante, au moins une partie des chiffres de la carte de paiement qui sont conservés en mémoire 102 ou une relation entre eux, par exemple leur somme, sont transmis au site tiers de protection 170 et servent à calculer l'information codée.

Préférentiellement, la communication entre le terminal 100 et le site tiers de protection 170 est cryptée ou sécurisée, selon des techniques connues.

Selon une variante non représentée, le site tiers de protection 170 crée un fichier de sauvegarde dans sa propre mémoire (non représentée) et y enregistre les informations reçues de la part du terminal 100. De manière préférentielle, un code d'intégrité est inséré dans le fichier et garantit que les données qui ont été enregistrées n'ont pas été modifiées depuis la création du fichier.

La figure 13 représente un écran de visualisation au cours de la mise en oeuvre du deuxième mode de réalisation du procédé objet de la présente invention, à la suite de l'opération 1109.

L'écran de visualisation 104 présente les même éléments que ceux illustrés en figure 10, auxquels sont superposées, dans la portion principale 1000, une fenêtre d'information complémentaire 1350 et une fenêtre de questionnaire 1360. La fenêtre d'information complémentaire 1350 comporte une indication 1310 indiquant que des données liées à la transaction ont été enregistrées, une information sur la loi applicable à la transaction, 1320, des informations légales de base 1330 et 1340 comportant, en particulier, une information sur la durée de la garantie légale 1330 et une information sur le délai légal maximal de réclamation concernant la transaction 1340.

La fenêtre de questionnaire 1360 comporte des textes indications permettant à l'utilisateur de renseigner des zones destinées à préciser des données liées à la transaction en cours. Dans l'exemple décrit et représenté, les renseignements suivants sont demandés à l'utilisateur :

- un code d'authentification, qui permet d'authentifier l'utilisateur de la carte de paiement ;
- un montant de paiement ;
- le nom du fournisseur ;
- l'objet ou le service obtenu en échange du paiement ;
- un délai d'alerte qui correspond à une date raisonnable ou l'utilisateur souhaite voir un message sur l'écran 104, par exemple à la mise en route de son terminal, message qui lui sert à vérifier si les obligations du fournisseur ont bien été honorées.

Les réponses à ce questionnaire sont mises en mémoire, localement et/ou par le biais d'un tiers de confiance, et, éventuellement, sont transmis (à l'exception du délai d'alerte) au site informatique distant 150.

Dans un autre mode de réalisation, tout ou partie de ces renseignements est automatiquement extrait des informations disponibles dans les pages reçues de la part du site informatique distant 150.

Selon une variante non représentée, la page fournie par le site informatique distant 150 comporte, de manière codée ou non, une information représentative de la date de la transaction ou un numéro de session et cette informations est mémorisée au cours de l'opération de sécurisation.

Selon d'autres variantes, les information mémorisées au cours de l'une des opérations 1109 ou 1209 sont représentatives des informations textuelles d'au moins une portion d'au moins une page fournie par le site informatique distant 150, portion qui a été affichée par l'écran 104, ou de l'une ou de plusieurs des informations suivantes :

- les informations textuelles des autres portions desdites pages,
- les informations textuelles des autres pages affichées par l'écran de visualisation 104 et fournies par le site informatique distant 150,
- des informations non textuelles (graphiques et images) desdites portions affichées,
- des informations non textuelles d'au moins deux pages fournies par le site informatique distant 150 et affichées par l'écran de visualisation 104,
- des informations non textuelles des autres pages fournies par le site informatique distant 150,
- des informations contextuelles, date, heure, autres sites visités précédemment, ... -

L'opération de sécurisation peut aussi comporter un affichage d'informations concernant la propriété intellectuelle relative à la transaction en cours, un clôture de la session, une transmission d'un message court sur un réseau de télécommunication, tel qu'un réseau téléphonique, par exemple mobile, ou un réseau de pageur, à un terminal de communication de l'utilisateur, message récapitulant les informations principales de la transaction en cours, une opération de transfert de données (date, montant du paiement, fournisseur) à un logiciel de tenue de comptabilité, personnelle ou professionnelle.

Un mode de réalisation du logiciel qui implémente le procédé objet de la présente invention, peut comporter, dans son code informatique, une partie d'un identifiant de moyen de paiement afin que ce logiciel soit associé à la carte de paiement. Ainsi, le logiciel peut être fourni par l'organisme financier qui a fourni la carte de paiement à l'utilisateur ou le logiciel peut être vendu sur un réseau de communication, tout en empêchant une copie illégale de ce logiciel d'être utilisée avec une autre carte de paiement. Dans ce dernier cas, une détection d'un moyen de paiement autre que celui qui est associé au logiciel peut provoquer l'affichage d'un message invitant l'utilisateur à acquérir une version du logiciel associée au moyen de paiement qu'il tente d'utiliser. Lorsqu'une commission est prévue pour la sécurisation de données ou avec un tiers de confiance, le logiciel put aussi provoquer un paiement pour payer cette commission.

L'opération de sécurisation peut aussi comporter la génération d'un certificat de transaction, mettant en oeuvre un tiers de confiance selon des techniques connues. Par

exemple, la détection du paiement peut provoquer l'émission par un tiers de confiance d'un identifiant de transaction qui est transmis à l'une ou l'autre des parties de la transaction en cours (par exemple le client), puis qui est retransmis entre les parties (par exemple au fournisseur) avant d'être utilisée pour obtenir le paiement.

Le procédé de l'invention peut être mis en oeuvre dans un logiciel comportant une fonction de fourniture d'une autorisation de paiement et, automatiquement, d'un identifiant d'un moyen de paiement. Ainsi, ce logiciel comporte une sécurisation conforme à ce qui est exposé ci-dessus. Dans ce cas, cependant, ce logiciel fonctionne, conformément à la présente invention en tâche de fond par rapport à la session de communication entre le terminal et le site informatique distant.

On observe que l'information mémorisée au cours de l'opération de sécurisation peut être limitée au montant de la transaction et à une date, ou à ces éléments et un identifiant du fournisseur, ou à une seule page reçue de la part du site informatique distant 150 (par exemple la page de paiement, qui devrait légalement, à terme, récapituler les informations contractuelles).

La manière dont les informations enregistrées au cours de l'une des opérations de sécurisation exposées ci-dessus sont relues et mises à disposition de l'utilisateur, d'un avocat ou de la justice, sont bien connues de l'homme du métier et ne sont donc pas détaillées ici. D'une manière préférentielle, ces données ne peuvent pas être modifiées sans que cela ne soit perceptible.

En figure 14 sont représentées les opérations effectuées pour la mise en oeuvre du procédé visé par la présente invention tel qu'illustré en figures 1 à 13 et 15.

Au cours d'une opération 1400, le logiciel mettant en oeuvre le procédé visé par la présente invention est installé.

Au cours de l'opération 1410, l'utilisateur sélectionne un mode de détection de préparation de paiement. Par exemple l'utilisateur donne les quatre premiers numéros d'une carte de paiement ou sélectionne que tout quadruplet de séquences de quatre chiffres ou une fonction d'un logiciel de paiement ou la sélection d'un icône dédié au paiement (non représenté) seront à détecter comme préparation d'un paiement en ligne.

Au cours de l'opération 1410, l'utilisateur sélectionne aussi les fonctions d'une opération de sécurisation, parmi celles qui sont exposées ci-dessus. L'opération de sécurisation comporte, au moins une opération de sauvegarde du montant du paiement. L'utilisateur peut aussi choisir un code secret, s'il souhaite être authentifié à chaque paiement

en ligne. L'utilisateur peut aussi choisir un tiers de confiance et un organisme financier. L'utilisateur désigne aussi un ou plusieurs logiciels de navigation sur un réseau de communication informatique tel qu'Internet. Le mode de fonctionnement sélectionné par l'utilisateur est mis en mémoire.

Au cours d'une opération 1420, à chaque mise en fonctionnement du terminal 100 ou à chaque lancement de l'un des logiciels de navigation désignés au cours de l'opération 1410, la fonction de détection de paiement et, en cas de détection, la fonction de sécurisation, sont mises en fonctionnement en tâche de fond. Des modes d'implémentation de l'opération 1420 sont décrits en regard des figures 11 et 12.

Au cours d'un test 1430, il est détecté si une période bancaire, par exemple la période facturation de l'utilisation d'une carte de paiement, a expiré, ou non. Si le résultat du test 1430 est négatif, l'opération 1420 est réitérée. Si le résultat du test 1430 est positif, un affichage et/ou une impression de tous les achats effectués au cours de la période bancaire considérée est effectuée au cours d'une opération 1440, puis l'opération 1420 est réitérée.

On observe que la détection de la préparation de paiement peut consister en une détection d'un paiement, par exemple, par détection de transmission, sur le bus 109, d'informations relative à un moyen de paiement ou par détection de mise en fonctionnement d'un logiciel ou d'une routine de paiement ou de comptabilisation.

Selon l'un de ses aspects, illustré en figure 15, le procédé objet de la présente invention détecte automatiquement (opération 1520), au cours d'une session de communication (ouverte au cours d'une opération 1500) entre un terminal informatique d'un utilisateur et un site informatique, sur un réseau tel qu'Internet, que l'utilisateur prépare un paiement par transmission, au cours de la session et par l'intermédiaire de son terminal, d'un identifiant d'un moyen de paiement (opération 1510). Par exemple, cette détection est effectuée en reconnaissant, parmi les chiffres saisis par l'intermédiaire d'un clavier du terminal, tout ou partie d'un numéro de carte de paiement ou de crédit (et/ou d'une date de péremption d'une telle carte, et/ou d'un numéro de compte bancaire et/ou d'une demande de certificat de transaction). Lorsque cette préparation de paiement est détectée, une opération 1530 de sécurisation dudit paiement.

Cette opération 1530 de sécurisation (soit, par exemple, de protection contre un usage abusif du consentement de l'utilisateur lié audit paiement) comporte au moins une opération 1537 de sauvegarde, en dehors du site informatique distant, du montant du paiement. L'opération de sauvegarde peut être effectuée en mémorisant ce montant, en l'imprimant ou

en le transmettant à distance. L'opération 1530 peut comporter, en outre, par exemple, une authentification de l'utilisateur 1531, une mise en mémoire des données échangées avec un format « texte » au cours de la session 1532, une communication à un tiers de confiance, tel qu'une banque auprès de laquelle le paiement doit être effectué, de données relatives au paiement (montant, fournisseur) 1533, un affichage de données juridiques 1534, l'impression d'informations relatives à la transaction ou d'un détail des paiements déjà effectués en ligne 1535, un cryptage de la transmission de données confidentielles 1536, un affichage de questionnaire en vue de son renseignement 1538.

Ceci permet à l'utilisateur d'avoir, au moins, une protection juridique car une trace de l'accord contractuel existe, et une protection financière car le paiement est limité au montant convenu.

La plupart des différents aspects de la présente invention peuvent être combinés pour la mise en oeuvre d'un procédé et d'un dispositif d'assistance à un utilisateur de réseau de communication.

Revendications

1. Procédé de communication caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une première session de communication avec un premier site d'un réseau de communication,

- une opération d'ouverture d'une deuxième session de communication avec un deuxième site dudit réseau de communication,

- une opération de transmission, audit deuxième site, d'informations relatives à la première session et

- une opération de réception, en provenance dudit deuxième site, d'informations relatives à la première session.

2. Procédé de communication selon la revendication 1, caractérisé en ce que ladite opération de transmission audit deuxième site comporte une opération de transmission automatique d'un identifiant dudit premier site.

3. Procédé de communication selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comporte une opération de mémorisation d'au moins une caractéristique d'une information confidentielle et ladite opération d'ouverture d'une deuxième session de communication comporte une opération de détection d'une caractéristique d'une information confidentielle dans des données à transmettre audit premier site.

4. Procédé de communication selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comporte une opération de transmission audit premier site d'informations basées sur des informations reçues en provenance dudit deuxième site.

5. Procédé de communication selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les informations reçues en provenance du deuxième site comporte une racine ou code générateur d'un identificateur de moyen de paiement.

6. Procédé de communication selon la revendication 5, caractérisé en ce qu'il comporte une opération de transmission dudit identificateur de moyen de paiement audit premier site.

7. Procédé de communication selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comporte une opération de mémorisation automatique de données reçues de la part du premier site au cours de ladite première session.

8. Procédé de communication selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comporte une opération de requête d'informations permettant de déterminer un identificateur de moyen de paiement à usage unique.

9. Procédé de communication caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication dite « deuxième » avec un terminal,

- une opération de réception en provenance dudit terminal d'une information relative à une session de communication dite « première » à laquelle participe ledit terminal et

- une opération de fourniture audit terminal d'informations relatives à la première session.

10. Procédé de communication selon la revendication 9, caractérisé en ce que les informations relatives à la première session comporte une racine ou code générateur permettant de définir un identificateur de moyen de paiement à usage unique.

11. Procédé de communication selon la revendication 10, caractérisé en ce qu'il comporte une opération de réception dudit identificateur, une opération de vérification de validité dudit identificateur, une opération de déclenchement de paiement et une opération d'invalidation dudit identificateur.

Revendications

1. Procédé de communication, caractérisé en ce qu'il comporte :

- une opération de détermination d'informations dites « à protéger » (303, 304),

- une opération d'ouverture d'une première session de communication entre un terminal informatique et un premier site d'un réseau de communication (702, 704),

- une opération de détection automatique d'une séquence de symboles correspondant à la transmision audit premier site d'une information à protéger audit premier site (706, 708) et

- lorsqu'une séquence de symboles est détectée, une opération automatique de sécurisation de ladite session (710 à 782), opération de sécurisation effectuée en dehors dudit premier site informatique, ladite opération de sécurisation comportant au moins l'une des opérations suivantes :

. une opération d'authentification d'un utilisateur,

. une opération de mémorisation de portions de pages provenant dudit site, en dehors dudit premier site et

. une opération de communication avec un deuxième site au cours de laquelle sont transmises des informations relatives au premier site.

2. Procédé de communication selon la revendication 1, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une deuxième session de communication avec un deuxième site dudit réseau de communication (710, 712),

- une opération de transmission, audit deuxième site, d'informations relatives à la première session et

- une opération de réception, en provenance dudit deuxième site, d'informations relatives à la première session.

3. Procédé de communication selon la revendication 2, caractérisé en ce que ladite opération de transmission audit deuxième site comporte une opération de transmission automatique d'un identifiant dudit premier site.

4. Procédé de communication selon l'une quelconque des revendications 2 ou 3, caractérisé en ce que:

- l'opération de détermination d'informations à protéger comporte une opération de mémorisation d'au moins une caractéristique d'une information confidentielle et

- ladite opération d'ouverture d'une deuxième session de communication comporte une opération de détection d'une caractéristique d'une information confidentielle dans des données à transmettre audit premier site.

5. Procédé de communication selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les informations reçues en provenance du deuxième site comporte une racine ou code générateur d'un identificateur de moyen de paiement.

6. Procédé de communication selon la revendication 5, caractérisé en ce qu'il comporte une opération de transmission dudit identificateur de moyen de paiement audit premier site.

7. Procédé de communication selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comporte une opération de mémorisation automatique de données reçues de la part du premier site au cours de ladite première session.

8. Procédé de communication selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comporte une opération de requête d'informations permettant de déterminer un identificateur de moyen de paiement à usage unique.

9. Procédé de communication selon l'une quelconque des revendications 1 à 8, caractérisé en ce que l'opération de détection automatique est effectuée en tâche de fond lorsque l'opération d'ouverture d'une première session de communication a eu lieu.

10. Dispositif de communication, caractérisé en ce qu'il comporte :

- un moyen de détermination d'informations dites « à protéger »,
- un moyen d'ouverture d'une première session de communication entre un terminal informatique et un premier site d'un réseau de communication,
- un moyen de détection automatique d'une séquence de symboles correspondant à la transmision audit premier site d'une information à protéger audit premier site et
- un moyen de sécurisation adapté, lorsqu'une séquence de symboles est détectée, à effectuer en dehors dudit site informatique, au moins l'une des opérations suivantes :

. une opération d'authentification d'un utilisateur,

. une opération de mémorisation de portions de pages provenant dudit site, en dehors dudit premier site et

. une opération de communication avec un deuxième site au cours de laquelle sont transmises des informations relatives au premier site.

ne permettent pas de constituer, avec la racine seule, un identificateur de moyen de paiement. Cette caractéristique est opposée au mode de fonctionnement décrit dans le brevet U.S. 5,883,810. La racine fournie par le site financier et/ou la détermination de l'identificateur du moyen de paiement à usage unique dépendent, préférentiellement, d'identificateurs de la transaction financière, comme son montant, l'identificateur de son bénéficiaire et/ou l'identificateur du site financier.

La racine fournie par le site financier peut être générée comme un certificat de transaction de la transaction en cours.

Le terminal 100 reçoit l'information destinée à participer à la détermination d'un identificateur de moyen de paiement à usage unique au cours de l'opération 772. Il détermine l'identificateur de moyen de paiement à usage unique au cours de l'opération 774, par exemple en mettant en oeuvre une fonction de calcul à sens unique du logiciel d'assistance, agissant sur l'information reçue de la part du site financier, d'un numéro de carte de paiement, d'un identificateur du site 150 et d'un montant de transaction. Eventuellement, un certification de transaction est aussi utilisé pour la détermination de l'identificateur de moyen de paiement à usage unique.

Dans l'exemple illustré en figure 7, au cours de l'opération 776, le terminal 100 et, au cours de l'opération 778, un site tiers de confiance 180 ouvrent une cinquième session de communication. Au cours d'une opération 780, le terminal 100 transmet des informations à séquestrer au site tiers de confiance. Ces informations sont des informations légales liées à la transaction effectuée avec le site tiers marchand. Au cours de l'opération 782, le site tiers de confiance 180 met en mémoire ces informations, éventuellement cryptées et dotées d'un certificat d'intégrité.

Dans l'exemple illustré en figure 7, au cours d'une opération 784, le site de protection 170 transmet un message de sécurisation au site tiers marchand pour confirmer que la transaction a été sécurisée.

On observe que en figure 7, les sites de protection 170, site financier et site tiers de confiance 180 ont été représentés comme des entités indépendantes. Cependant, dans d'autres modes de réalisation du procédé de la présente invention, deux ou trois de ces sites sont confondus en une seule entité.

On observe que le site dit financier peut ne servir que d'intermédiaire entre les parties à la transaction (l'utilisateur et le site tiers marchand) et faire effectuer le paiement par un autre organisme financier, après lui avoir fourni un identifiant de l'utilisateur ou d'un moyen

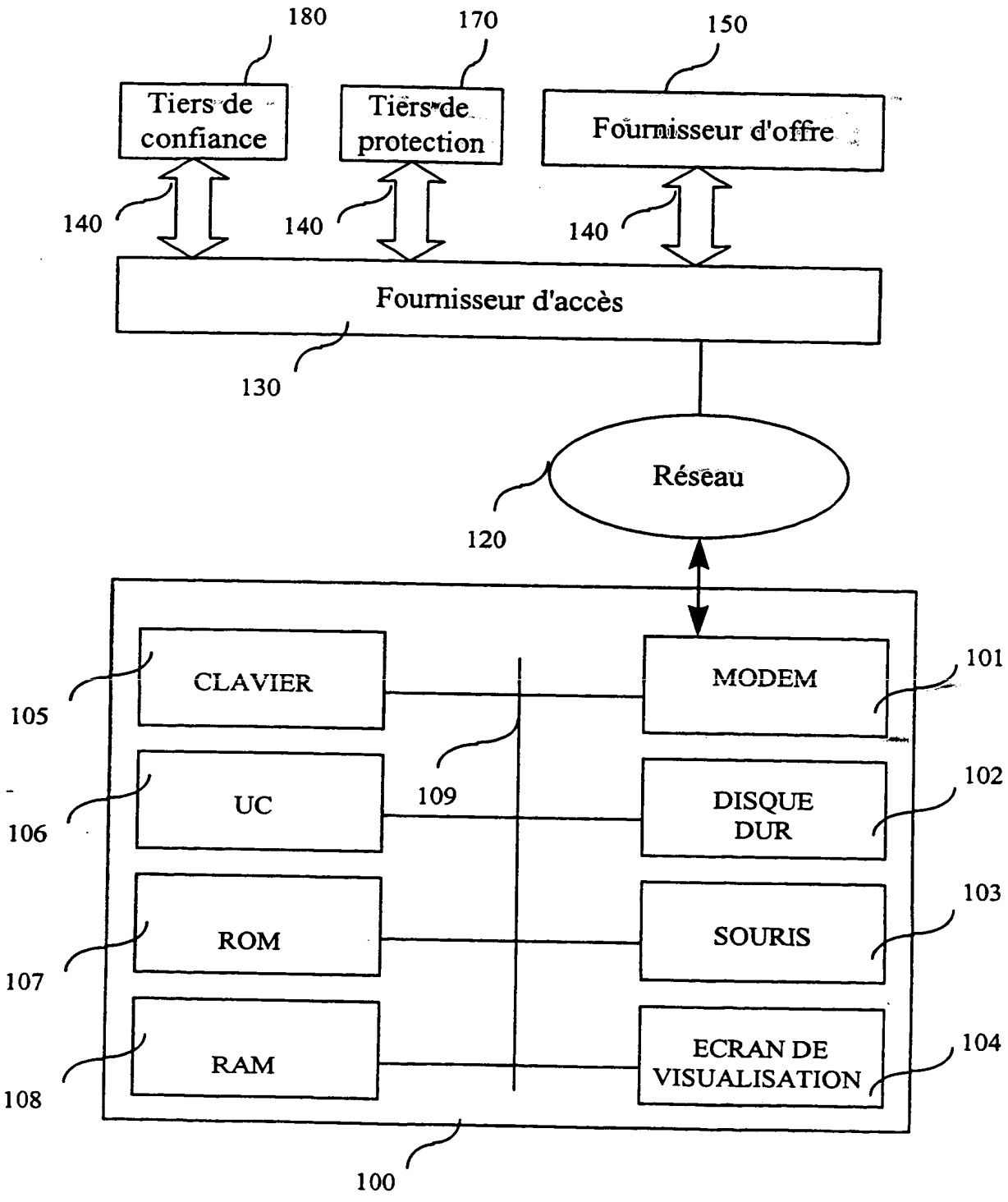
180
170
150
Tiers de confiance
Tiers de protection
Fournisseur d'offre
140
140
140
Fournisseur d'accès
130
Réseau
120
CLAVIER
105
MODEM
101
UC
106
109
DISQUE DUR
102
ROM
107
SOURIS
103
RAM
108
ECRAN DE VISUALISATION
104
100

Fig. 1

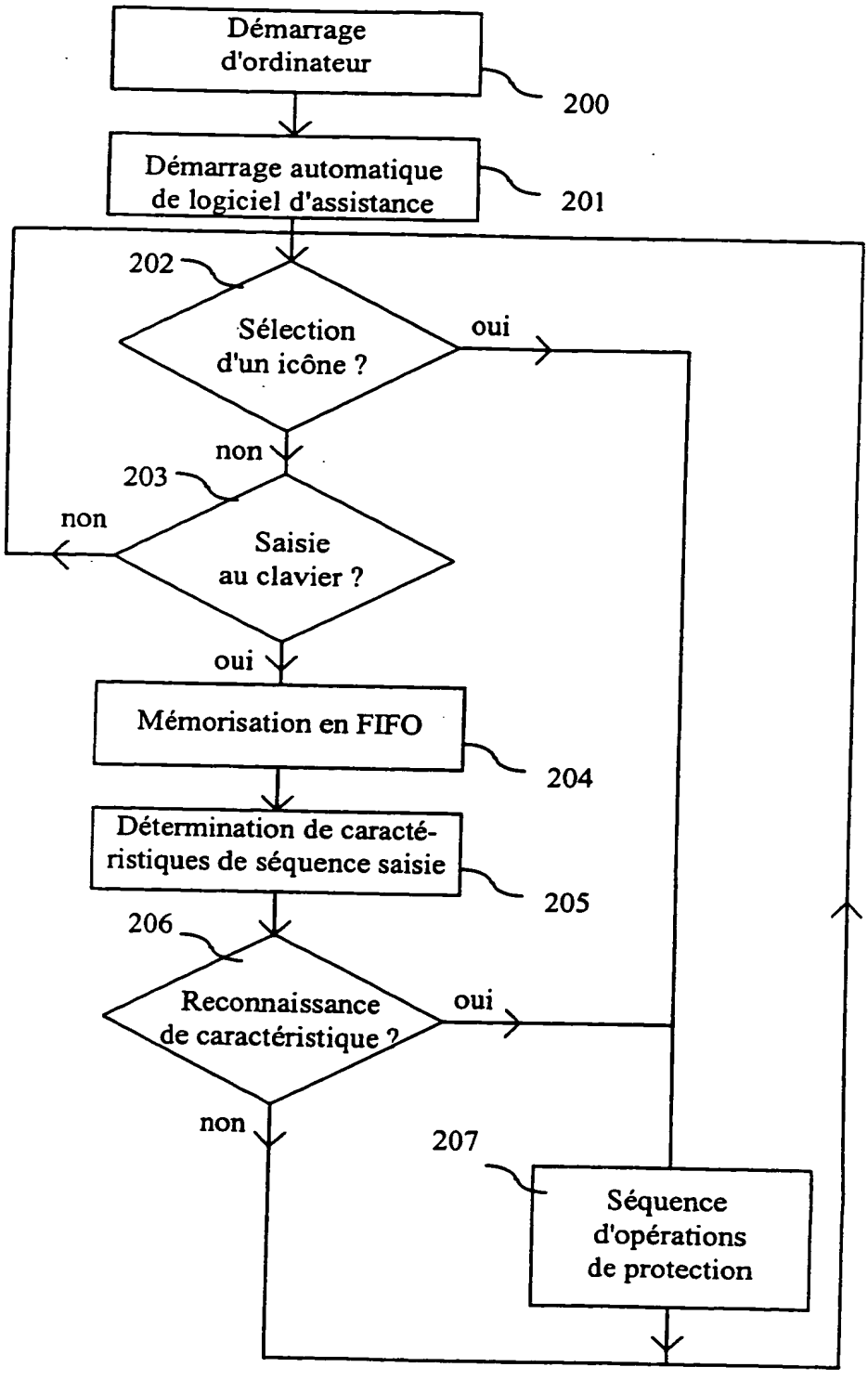
Démarrage d'ordinateur
200
Démarrage automatique de logiciel d'assistance
201
202
Sélection d'un icône ?
oui
non
203
Saisie au clavier ?
non
oui
Mémorisation en FIFO
204
Détermination de caractéristiques de séquence saisie
205
206
Reconnaissance de caractéristique ?
oui
non
207
Séquence d'opérations de protection

Fig. 2

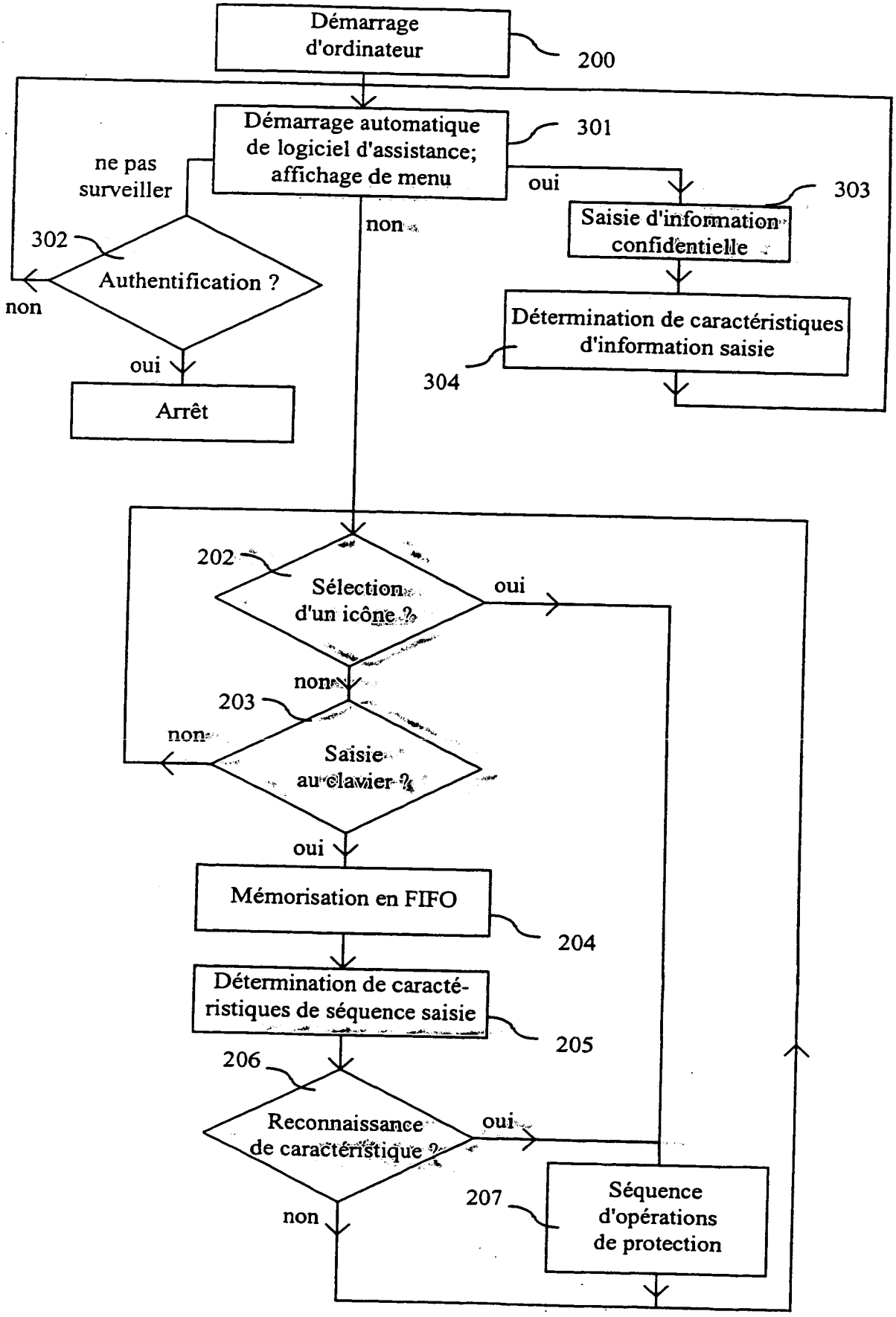
Démarrage d'ordinateur
200
Démarrage automatique de logiciel d'assistance; affichage de menu
301
ne pas surveiller
oui
303
non
Saisie d'information confidentielle
302
Authentification ?
non
oui
Détermination de caractéristiques d'information saisie
304
Arrêt
202
Sélection d'un icône ?
oui
non
203
non
Saisie au clavier ?
oui
Mémorisation en FIFO
204
Détermination de caractéristiques de séquence saisie
205
206
Reconnaissance de caractéristique ?
oui
non
207
Séquence d'opérations de protection

Fig. 3

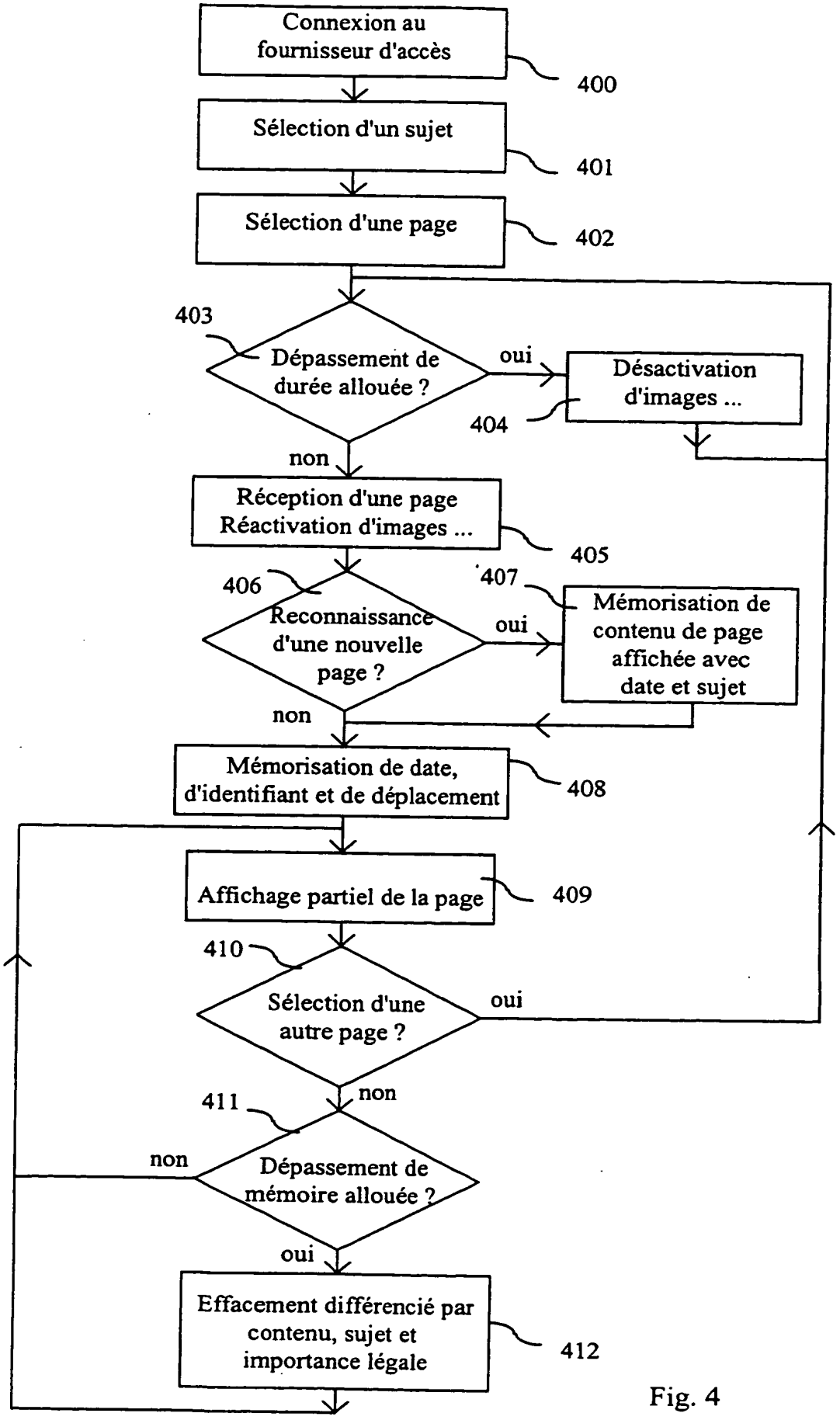
Connexion au fournisseur d'accès
400
Sélection d'un sujet
401
Sélection d'une page
402
403
Dépassement de durée allouée ?
oui
Désactivation d'images ...
404
non
Réception d'une page Réactivation d'images ...
405
406
Reconnaissance d'une nouvelle page ?
407
oui
Mémorisation de contenu de page affichée avec date et sujet
non
Mémorisation de date, d'identifiant et de déplacement
408
Affichage partiel de la page
409
410
Sélection d'une autre page ?
oui
non
411
Dépassement de mémoire allouée ?
non
oui
Effacement différencié par contenu, sujet et importance légale
412

Fig. 4

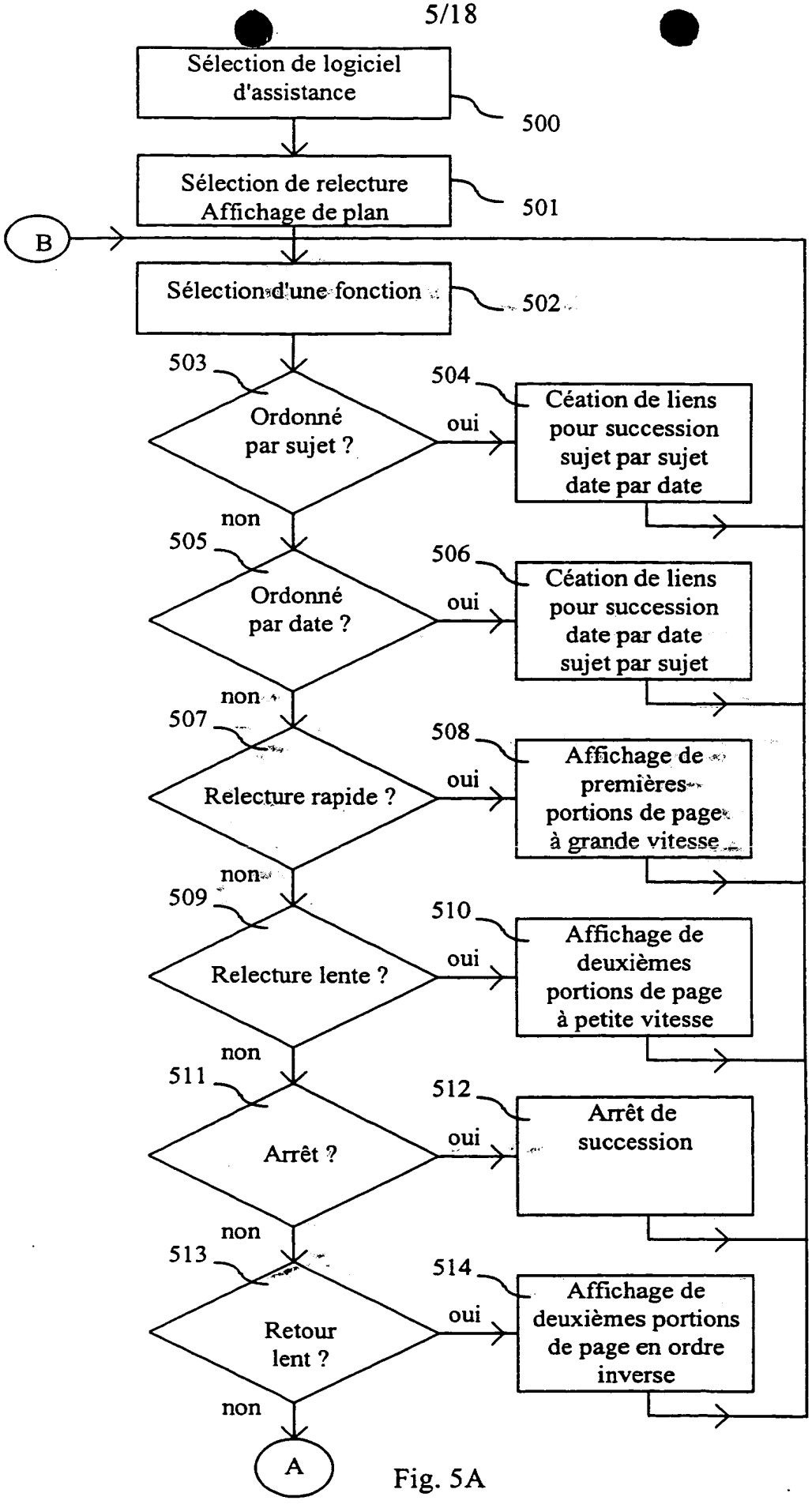
Sélection de logiciel d'assistance
500
Sélection de relecture Affichage de plan
501
B
Sélection d'une fonction
502
503
Ordonné par sujet ?
oui
504
Céation de liens pour succession sujet par sujet date par date
non
505
Ordonné par date ?
oui
506
Céation de liens pour succession date par date sujet par sujet
non
507
Relecture rapide ?
oui
508
Affichage de premières portions de page à grande vitesse
non
509
Relecture lente ?
oui
510
Affichage de deuxièmes portions de page à petite vitesse
non
511
Arrêt ?
oui
512
Arrêt de succession
non
513
Retour lent ?
oui
514
Affichage de deuxièmes portions de page en ordre inverse
non
A

Fig. 5A

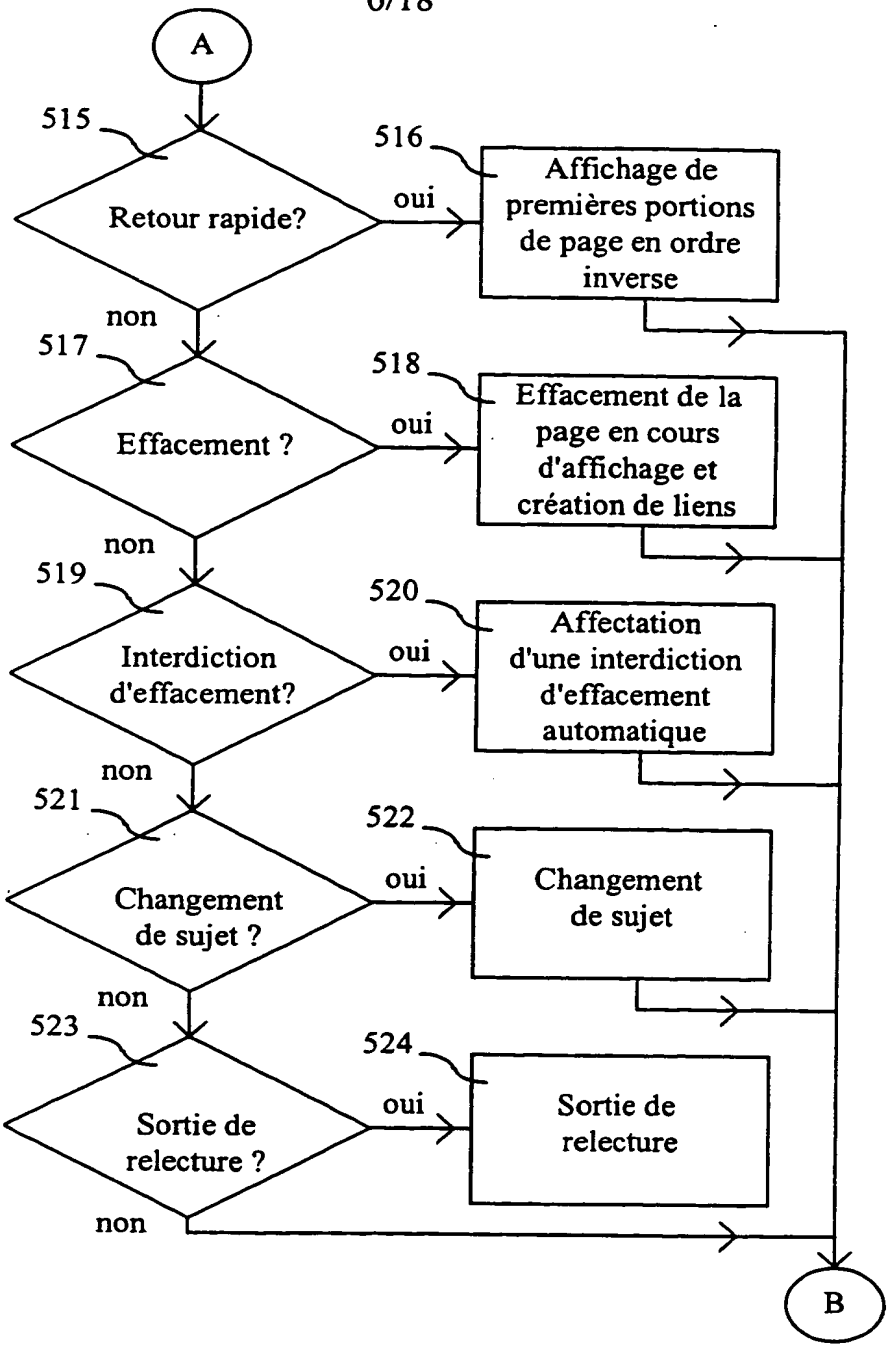
A
515
Retour rapide?
oui
516
Affichage de premières portions de page en ordre inverse
non
517
Effacement ?
oui
518
Effacement de la page en cours d'affichage et création de liens
non
519
Interdiction d'effacement?
oui
520
Affectation d'une interdiction d'effacement automatique
non
521
Changement de sujet ?
oui
522
Changement de sujet
non
523
Sortie de relecture ?
oui
524
Sortie de relecture
non
B

Fig. 5B

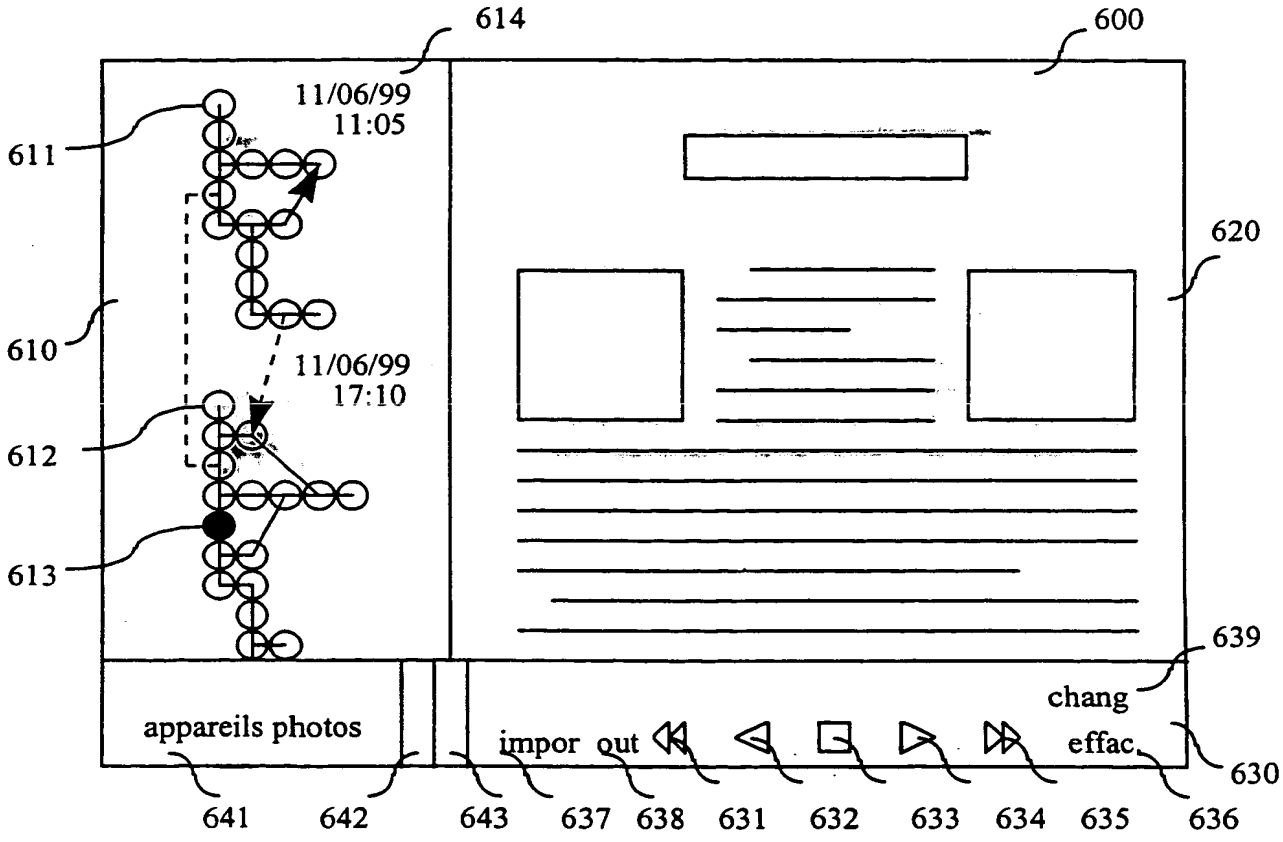
614
600
11/06/99
11:05
611
620
610
11/06/99
17:10
612
613
639
chang
appareils photos
impor
out
effac
630
641
642
643
637
638
631
632
633
634
635
636

Fig 6

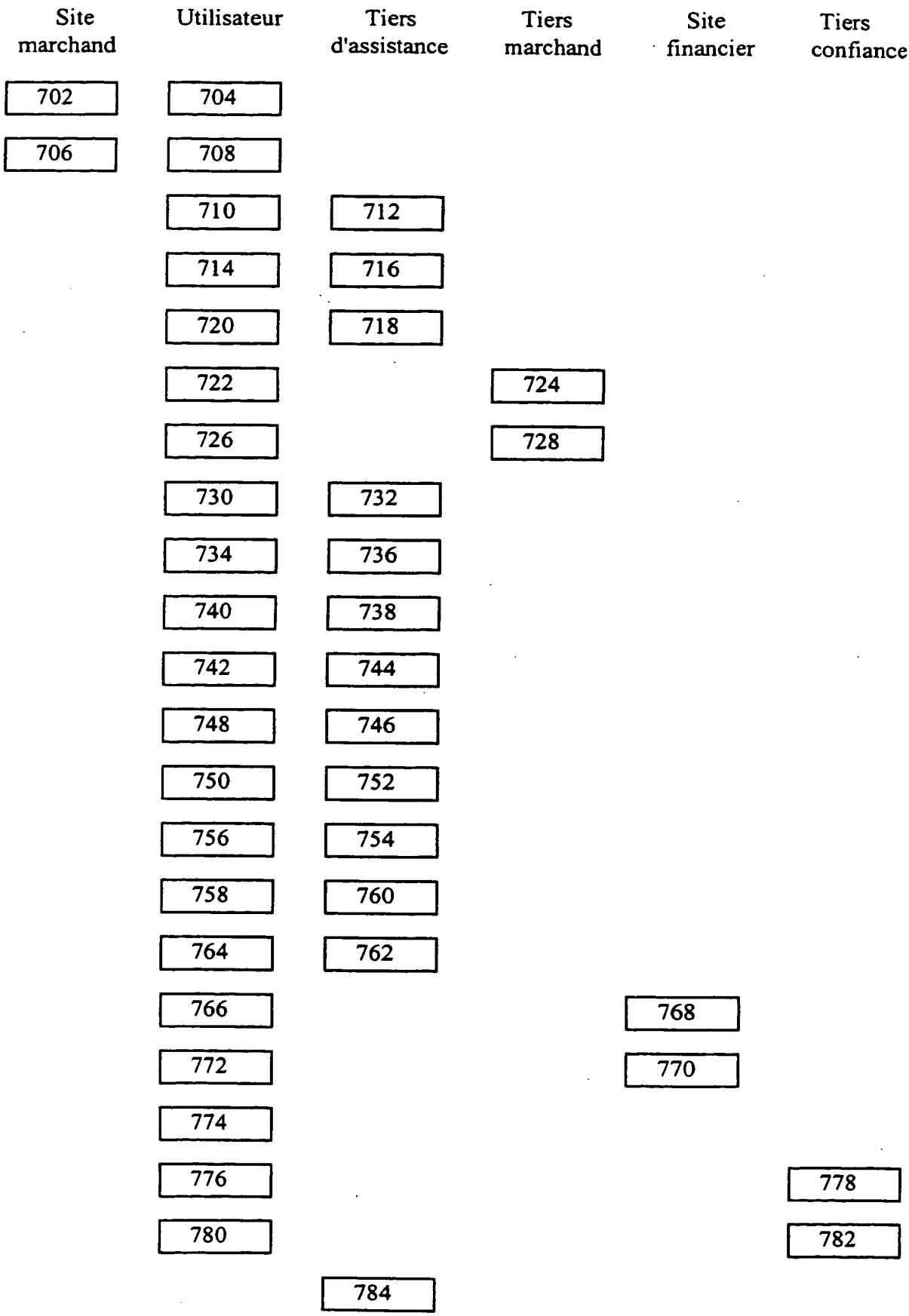
Site marchand
Utilisateur
Tiers d'assistance
Tiers marchand
Site financier
Tiers confiance
702
704
706
708
710
712
714
716
720
718
722
724
726
728
730
732
734
736
740
738
742
744
748
746
750
752
756
754
758
760
764
762
766
768
772
770
774
776
778
780
782
784

Fig. 7

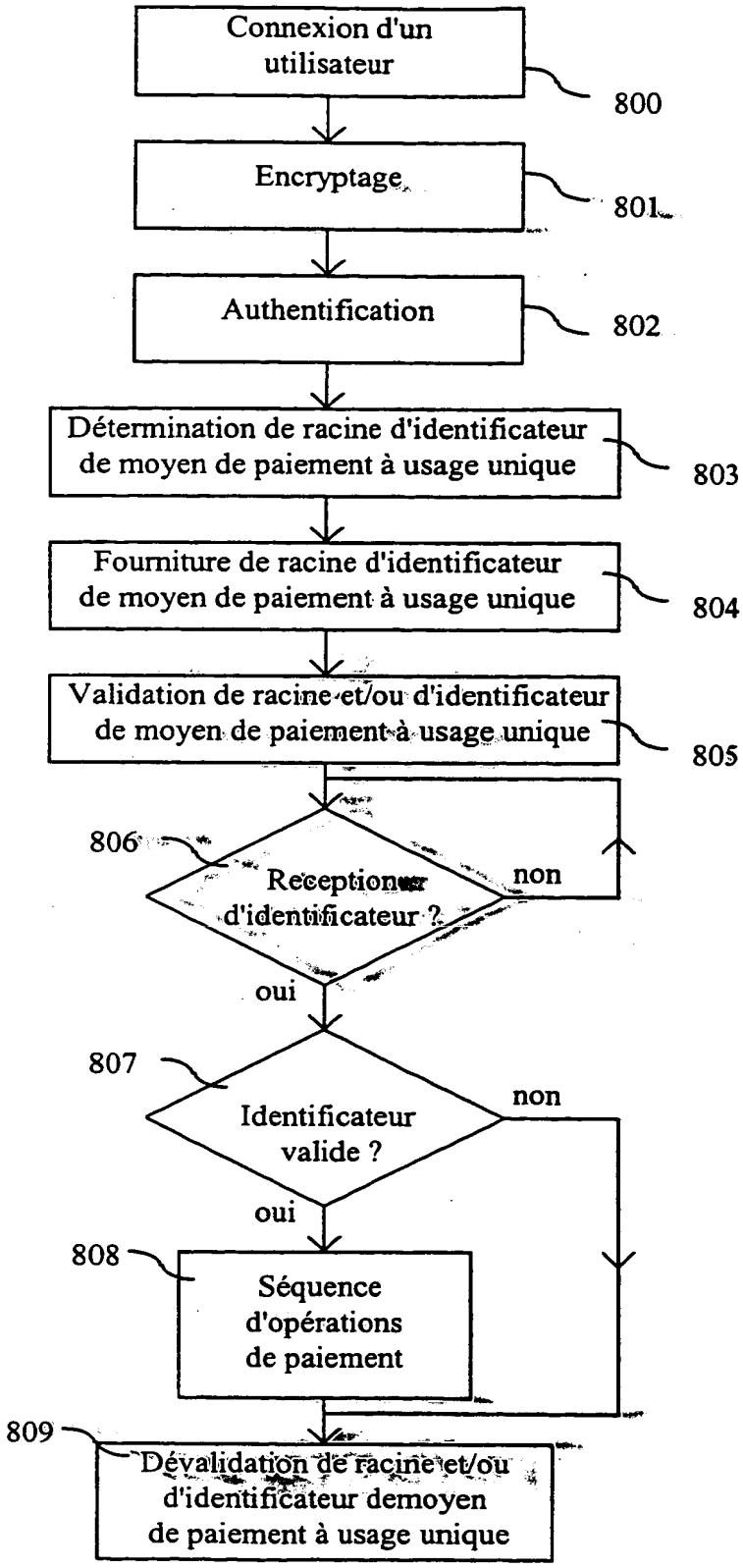
Connexion d'un utilisateur
800
Encryptage
801
Authentification
802
Détermination de racine d'identificateur de moyen de paiement à usage unique
803
Fourniture de racine d'identificateur de moyen de paiement à usage unique
804
Validation de racine et/ou d'identificateur de moyen de paiement à usage unique
805
806
Reception d'identificateur ?
non
oui
807
Identificateur valide ?
non
oui
808
Séquence d'opérations de paiement
809
Dévalidation de racine et/ou d'identificateur demoyen de paiement à usage unique

Fig. 8

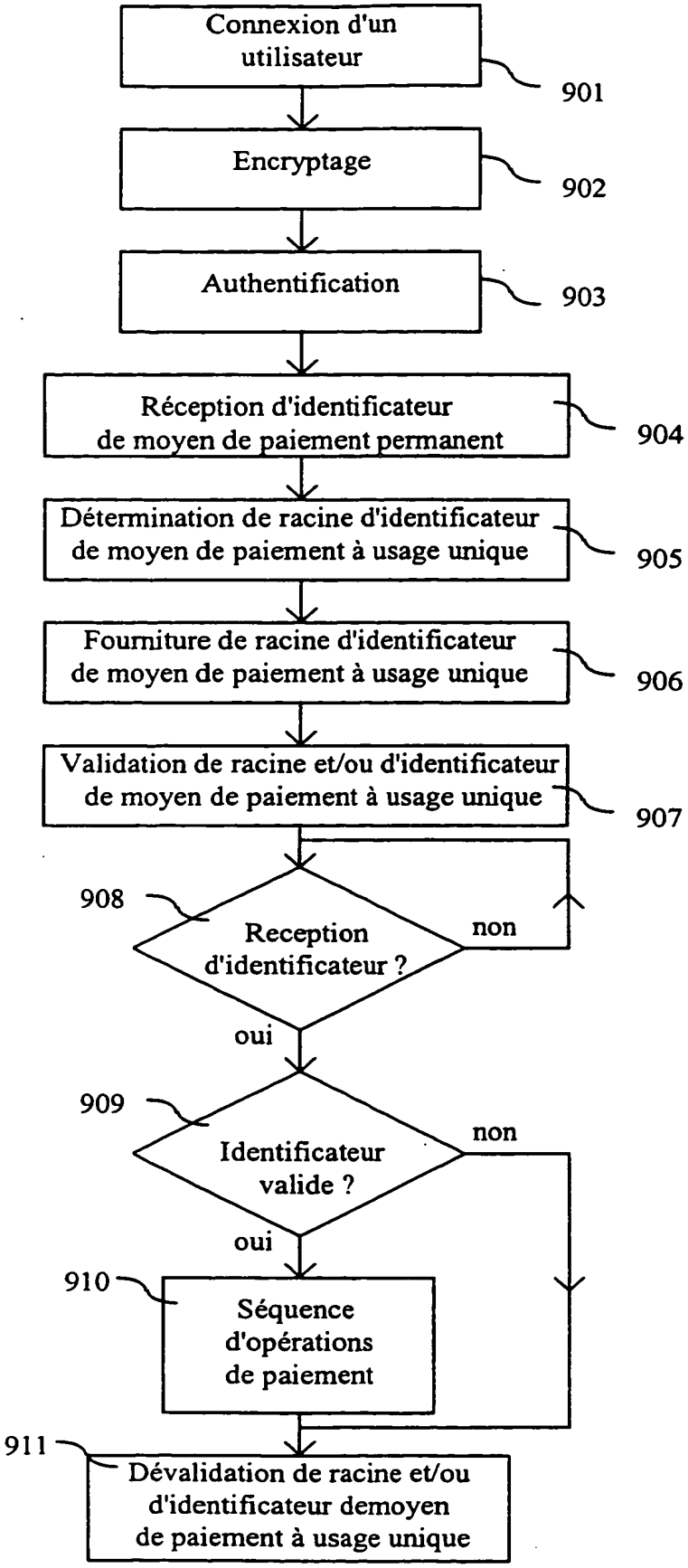
Connexion d'un utilisateur
901
Encryptage
902
Authentification
903
Réception d'identificateur de moyen de paiement permanent
904
Détermination de racine d'identificateur de moyen de paiement à usage unique
905
Fourniture de racine d'identificateur de moyen de paiement à usage unique
906
Validation de racine et/ou d'identificateur de moyen de paiement à usage unique
907
908
Reception d'identificateur ?
non
oui
909
Identificateur valide ?
non
oui
910
Séquence d'opérations de paiement
911
Dévalidation de racine et/ou d'identificateur demoyen de paiement à usage unique

Fig. 9

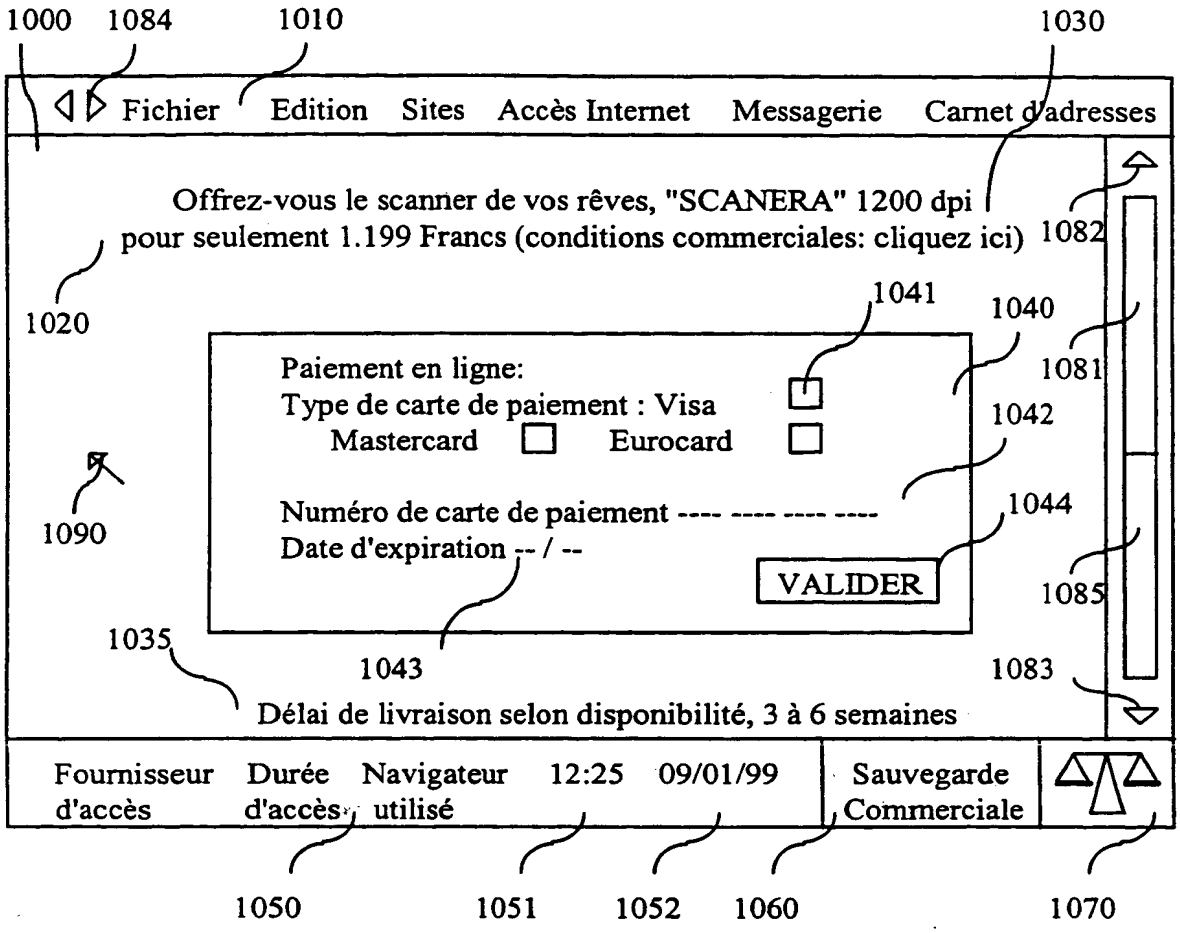
1000
1084
1010
1030
Fichier
Edition
Sites
Accès Internet
Messagerie
Carnet d'adresses
Offrez-vous le scanner de vos rêves, "SCANERA" 1200 dpi
pour seulement 1.199 Francs (conditions commerciales: cliquez ici)
1082
1020
1041
1040
1081
Paiement en ligne:
Type de carte de paiement : Visa
Mastercard
Eurocard
1042
1090
Numéro de carte de paiement ---- ---- ---- ----
1044
Date d'expiration -- / --
VALIDER
1085
1035
1043
1083
Délai de livraison selon disponibilité, 3 à 6 semaines
Fournisseur d'accès
Durée d'accès
Navigateur utilisé
12:25
09/01/99
Sauvegarde Commerciale
1050
1051
1052
1060
1070

Fig. 10

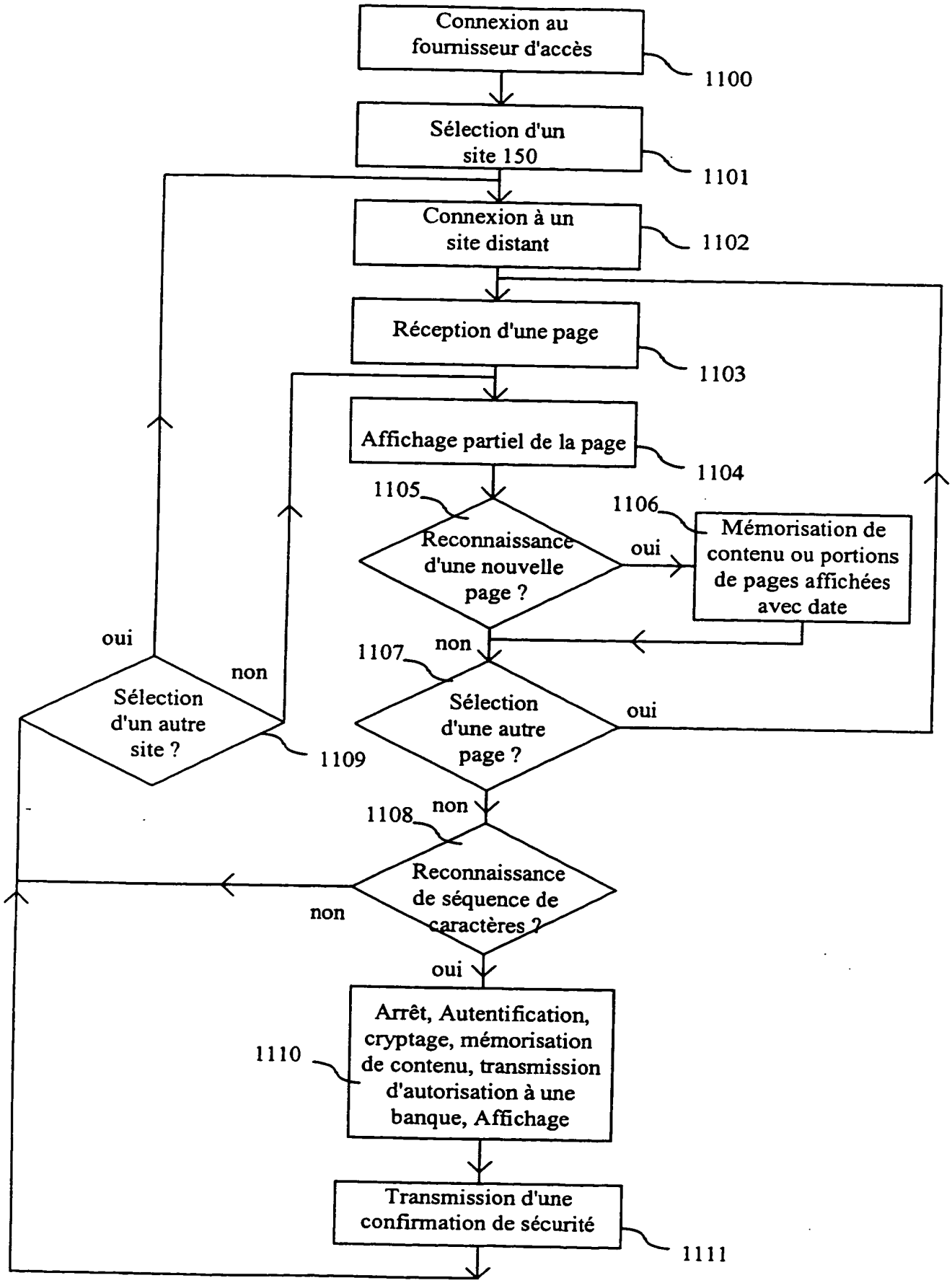
Connexion au fournisseur d'accès
1100
Sélection d'un site 150
1101
Connexion à un site distant
1102
Réception d'une page
1103
Affichage partiel de la page
1104
1105
Reconnaissance d'une nouvelle page ?
oui
1106
Mémorisation de contenu ou portions de pages affichées avec date
non
1107
Sélection d'une autre page ?
oui
non
Sélection d'un autre site ?
oui
non
1109
1108
Reconnaissance de séquence de caractères ?
non
oui
1110
Arrêt, Autentification, cryptage, mémorisation de contenu, transmission d'autorisation à une banque, Affichage
Transmission d'une confirmation de sécurité
1111

Fig. 11

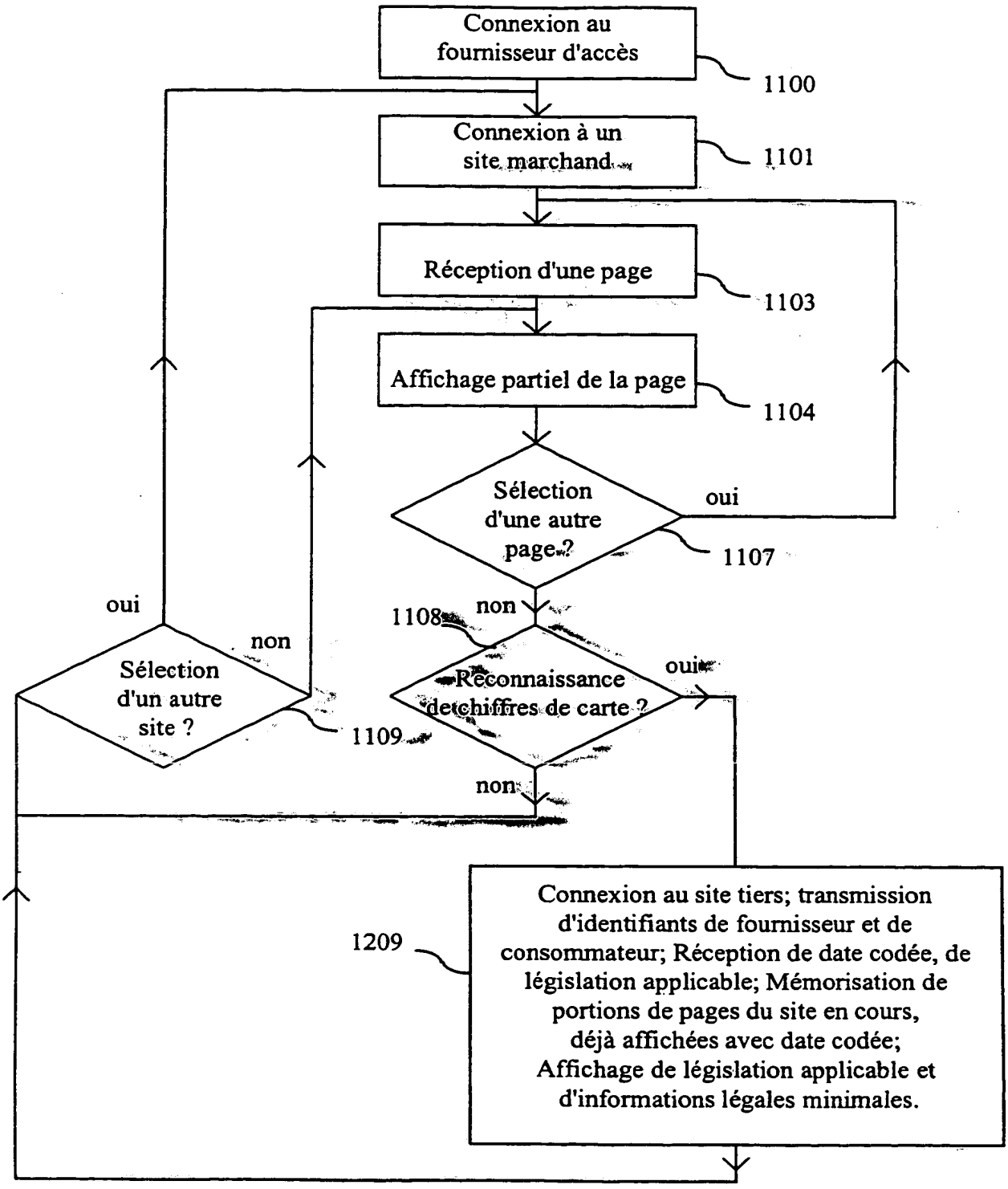
Connexion au fournisseur d'accès
1100
Connexion à un site marchand
1101
Réception d'une page
1103
Affichage partiel de la page
1104
Sélection d'une autre page ?
1107
oui
non
1108
Reconnaissance de chiffres de carte ?
oui
non
Sélection d'un autre site ?
1109
oui
non
1209
Connexion au site tiers; transmission d'identifiants de fournisseur et de consommateur; Réception de date codée, de législation applicable; Mémorisation de portions de pages du site en cours, déjà affichées avec date codée; Affichage de législation applicable et d'informations légales minimales.

Fig. 12

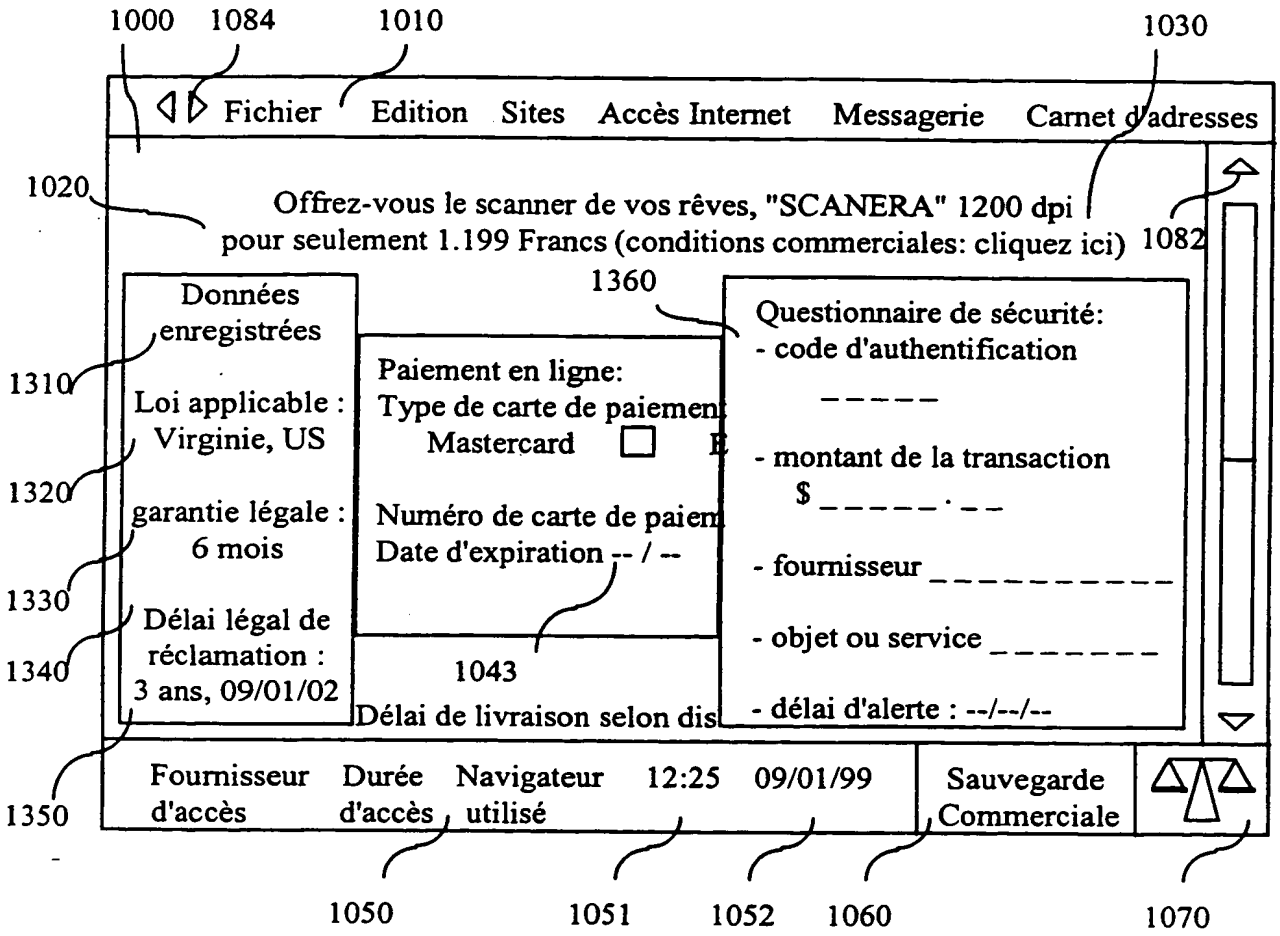
1000
1084
1010
1030
Fichier
Edition
Sites
Accès Internet
Messagerie
Carnet d'adresses
1020
Offrez-vous le scanner de vos rêves, "SCANERA" 1200 dpi
pour seulement 1.199 Francs (conditions commerciales: cliquez ici)
1082
1360
Données enregistrées
1310
Loi applicable : Virginie, US
1320
garantie légale : 6 mois
1330
Délai légal de réclamation : 3 ans, 09/01/02
1340
Paiement en ligne:
Type de carte de paiement
Mastercard
Numéro de carte de paiem
Date d'expiration -- / --
1043
Délai de livraison selon dis
Questionnaire de sécurité:
- code d'authentification
- montant de la transaction
$ _ _ _ _ _ . _ _
- fournisseur _ _ _ _ _ _ _ _ _ _
- objet ou service _ _ _ _ _ _ _
- délai d'alerte : --/--/--
1350
Fournisseur d'accès
Durée d'accès
Navigateur utilisé
12:25
09/01/99
Sauvegarde Commerciale
1050
1051
1052
1060
1070

Fig. 13

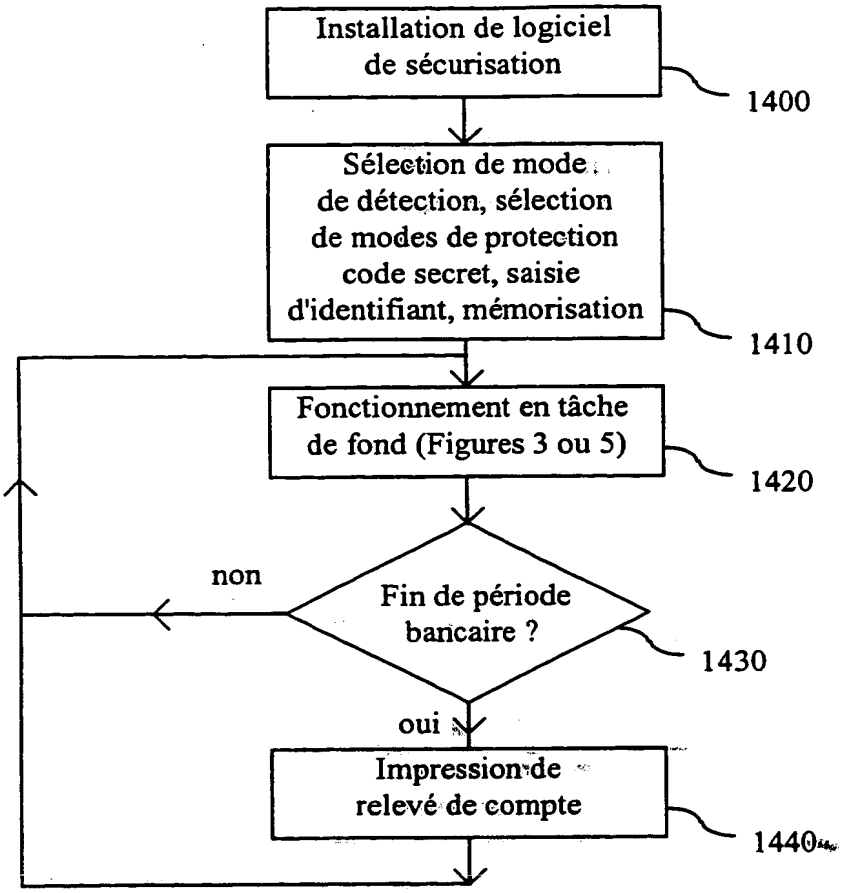
Installation de logiciel de sécurisation
1400
Sélection de mode de détection, sélection de modes de protection code secret, saisie d'identifiant, mémorisation
1410
Fonctionnement en tâche de fond (Figures 3 ou 5)
1420
non
Fin de période bancaire ?
1430
oui
Impression de relevé de compte
1440

Fig. 14

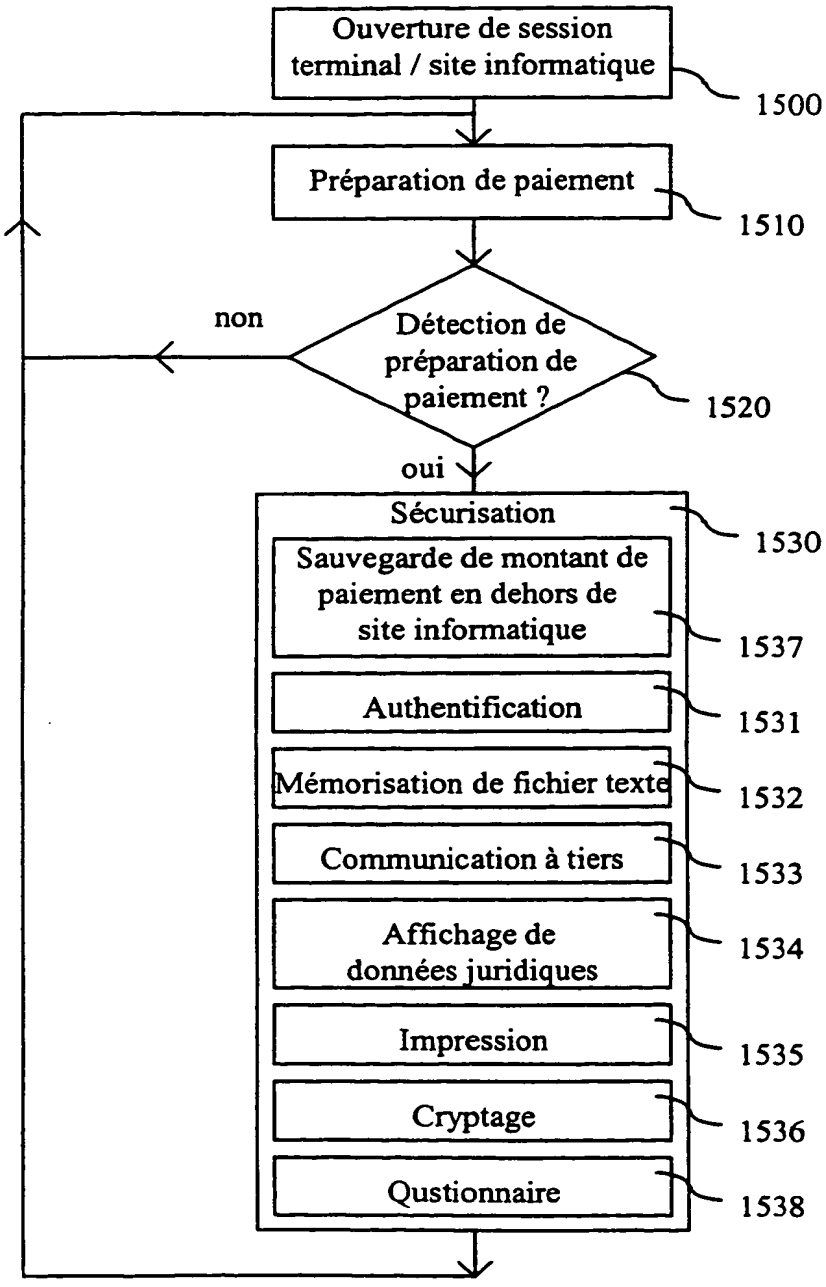
Ouverture de session terminal / site informatique
1500
Préparation de paiement
1510
non
Détection de préparation de paiement ?
1520
oui
Sécurisation
1530
Sauvegarde de montant de paiement en dehors de site informatique
1537
Authentification
1531
Mémorisation de fichier texte
1532
Communication à tiers
1533
Affichage de données juridiques
1534
Impression
1535
Cryptage
1536
Qustionnaire
1538

Fig. 15

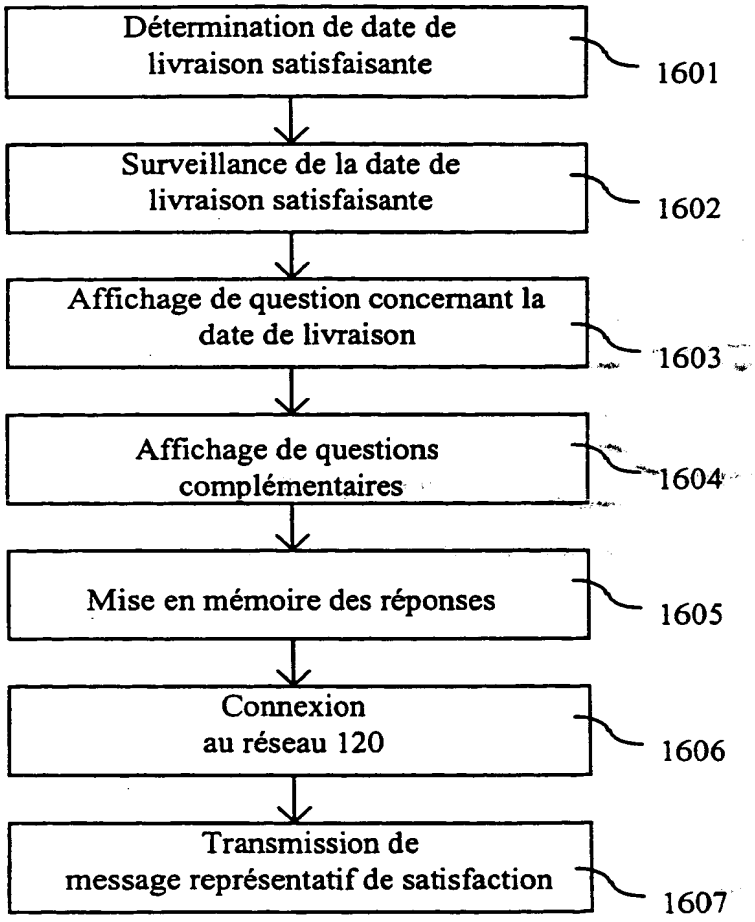
Détermination de date de livraison satisfaisante
1601
Surveillance de la date de livraison satisfaisante
1602
Affichage de question concernant la date de livraison
1603
Affichage de questions complémentaires
1604
Mise en mémoire des réponses
1605
Connexion au réseau 120
1606
Transmission de message représentatif de satisfaction
1607

Fig. 16

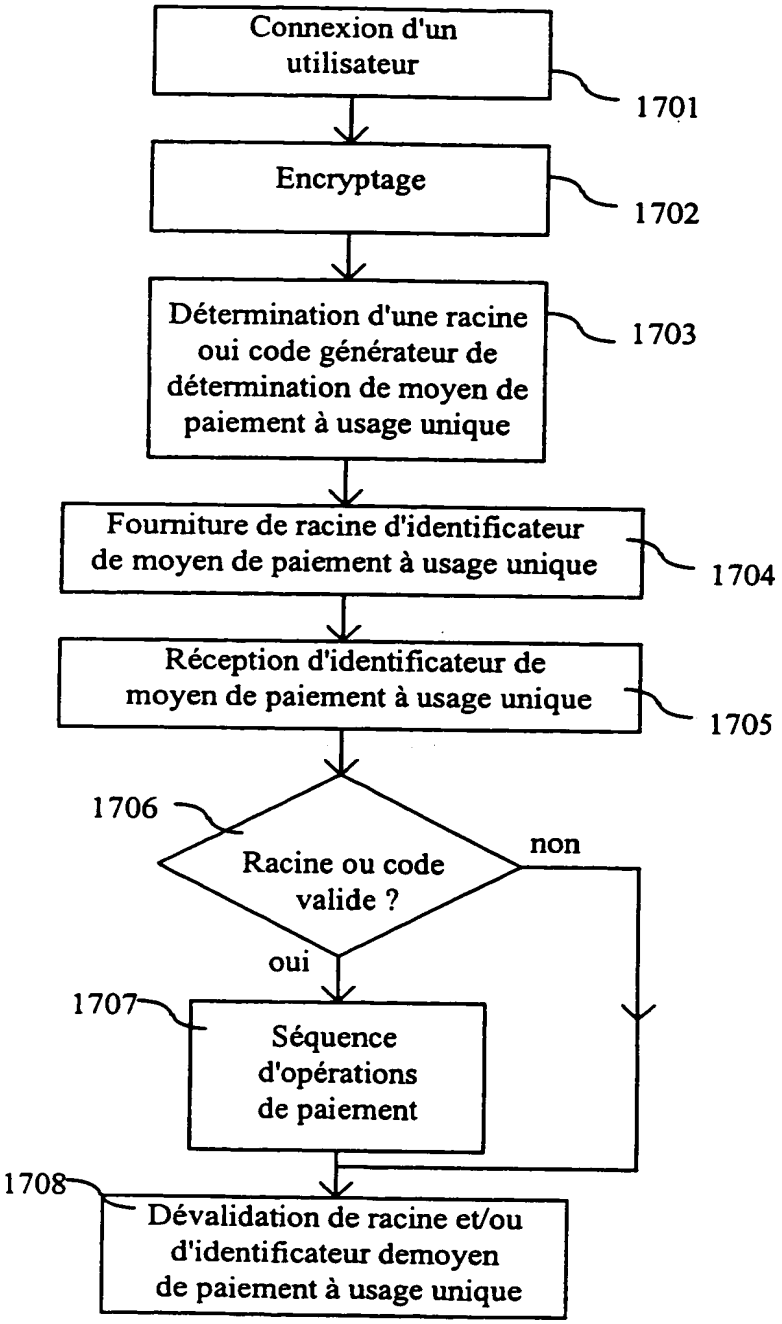
Connexion d'un utilisateur
1701
Encryptage
1702
Détermination d'une racine oui code générateur de détermination de moyen de paiement à usage unique
1703
Fourniture de racine d'identificateur de moyen de paiement à usage unique
1704
Réception d'identificateur de moyen de paiement à usage unique
1705
1706
Racine ou code valide ?
non
oui
1707
Séquence d'opérations de paiement
1708
Dévalidation de racine et/ou d'identificateur demoyen de paiement à usage unique

Fig. 17